The Joy of Numbers: Stalking the Big Primes

Professor Tom Marley
Department of Mathematics
University of Nebraska – Lincoln

Fall Semester, 2008

Contents

1. Divisibility in the integers 1
2. More on divisibility 2
3. Greatest Common Divisors 4
4. The Division Theorem 6
5. Linear Combinations 9
6. The equation $ax + by = m$ 12
7. A first look at primes 15
8. More on primes 20
9. Mathematical Induction 23
10. The E-Zone 27
11. The Fundamental Theorem of Arithmetic 30
12. More on Congruences 33
13. Fast Exponentiation 35
14. More on Exponentiation 38
15. Cancellation modulo m 41
16. Powers modulo m 43
17. Fermat's Theorem 44
18. More on Fermat's Theorem and inverses modulo m 46
19. A first look at cryptography 52
20. Public Key Cryptography and RSA 56
21. More on RSA 59
22. The Euler ϕ-function 62
23. The Chinese Remainder Theorem 66
24. More on the Chinese Remainder Theorem 69
25. The Euler ϕ-function, revisited 71

Appendix A. Using Maple 73
Appendix B. Projects 75
Appendix C. Take-Home Test 1 77
Appendix D. Take-Home Test 2 79
Appendix E. Take-Home Test 3 81
Appendix F. Take-Home Test 4 83
Appendix G. Take-Home Test 5 85
Appendix H. Take-Home Test 6 87

The Joy of Numbers: Stalking the Big Primes
Professor Tom Marley – Fall 2008
Course Information Sheet

Course Description:: You will experience the beauty and power of mathematics by exploring the properties of the integers and some of their modern applications. Number Theory, the branch of mathematics which focuses on the integers, is one of the oldest and most beautiful areas of mathematics, as well as one of the hottest areas of current research and applications. A central theme of the course will be the search for big primes, a problem as old as ancient Greece, and as new as today's newspaper. Part of our fascination with the integers is that they are the simplest of all mathematical objects, known to virtually every culture in recorded history, but problems involving them can be extremely challenging.

You will construct much of the content of the course, with questions from the instructor to stimulate your thinking. By considering concrete examples and looking for common threads or patterns, you will make conjectures (guesses based on good examples and data) and then try to verify or disprove them. You will gain facility and become confident that you can *do* mathematics and you will experience the joy of discovering hidden patterns and mathematical truths. You will gain an appreciation of the achievements of some of the great masters of the subject and you will see how much of our modern electronic world depends on Number Theoretic ideas.

As we investigate those most basic of mathematical objects, the integers, much of our emphasis will be on their building blocks, the primes. Our goal will be to discover the key facts about the integers and especially the primes that are needed for many of the modern applications of Number Theory. As we establish these key facts, we shall see how they are used in everything from card shuffling to shopping on the Internet.

Instructor: : Professor Tom Marley

Office: Avery 305.

Office Hours: 1:00 - 2:30 Mondays, 2:00 - 3:00 on Wednesdays, or by appointment.

Phone: 472–7250.

Email: `tmarley1@math.unl.edu` This is the most reliable way to reach me, and is, in particular, much better than phone messages.

Web Page: `http://www.math.unl.edu/~tmarley1`

Text: : There will be no text. At the beginning of each class, I will distribute notes summarizing the discussion of the previous class. You will need to have a good notebook in which to record your work and keep these notes. I recommend buying a three-ring binder.

Homework: : Daily homework problems will be assigned and you will be expected to have prepared them for the next class. They are not to be written up to be handed in, but you are expected to be prepared to present your solution in class when called upon. Collaboration is both allowed and strongly encouraged on the daily homework problems. One of the best ways to learn is to try

to explain what you are doing to someone else. The most important part of this course is the homework problems. Mathematics can be learned only by *doing* mathematics, and to succeed in this course, you must do the homework on a regular basis. Reread the previous two sentences. This message there cannot be overemphasized!

Participation: : Each day I will randomly call upon several of you to present to the class your attempts at solutions to the homework problems assigned the previous class period. You are expected to be ready. Class participation will influence your final grade, as described in the section on Grading below.

Questions: : There are no dumb questions. If you don't understand something that I or one of your classmates is saying, stop us and ask for another explanation. If you have a question, there are surely others with the same question who may initially be too shy to ask. So speak up! You will be doing a service for your more reticent classmates.

Good Manners: : In doing mathematics, or almost anything worth doing in life, one is going to make many errors and false starts while becoming more proficient. Think, for example, of learning to play a musical instrument or learning an athletic skill. We want to establish a classroom atmosphere where the inevitable false starts and mistakes become an opportunity to learn and to get better – not an opportunity for embarrassment. Thus, please be constructive and polite in questioning your colleagues in class.

Tests: : There will be no in-class tests. There will be six take-home tests. Three of these will be *collaborative*, (i.e., collaboration with other students is allowed and encouraged) and three will be *solo*, which means you work alone and no collaboration of any kind is allowed. The scheduled dates for the take-home tests are:

Given Out	Due	Type
September 4	September 11	Collaborative
September 18	September 25	Solo
October 2	October 9	Collaborative
October 23	October 30	Solo
November 6	November 13	Collaborative
November 20	December 4	Solo

Throughout this course and especially on the tests, I am more interested is seeing what you can do when given the time to reflect and think creatively, rather than having you repeat back information. Thus you may find some of the test problems somewhat challenging and frustrating at first. Don't be discouraged. I want you to expand your thinking and to become more creative, to work like a scientist or mathematician in exploring the unknown. I don't expect you to be able to do all the problems.

Final Exam:: There is no final exam for this course.

Class Project: : Each student will be required to participate in a group project (2-3 students per group). These projects will have both a written and an oral component. The last three classes or so and the final exam period (if necessary) will be reserved for oral presentations, and the written part is to

be turned in the day the oral part is presented. These projects can be based on interesting problems or applications that were considered in class, but which were not resolved, or they can be chosen from a list of topics I will distribute in early October, or they can be on almost any topic (related to the course material) which has captured your interest. All topics must be approved in advance by me and all projects must be completed by the assigned presentation date. All participants in a group project will get the same grade on that work, so it is important that each person in the group participate fully and equally. Attendance during the project presentations is **mandatory** for all members of the class.

Extensions: : There will be **NO** extensions. All work is due on the day it is due. Late work (regardless of reason) will be severely penalized. You know now when everything in this class will be due. Plan ahead.

Grading: : Final grades will be determined as follows:

class participation – 20%
take-home tests – 60%
project – 20%

Honor Code: : I will be very explicit about when you may collaborate and when I expect the work you hand in to be yours alone. I will assume that you will adhere to the UNL Policy on Academic Honesty.

Joy of Numbers – Project Presentation Schedule

The schedule for the project presentations is:

Date	Group	Topic
Tuesday, December 9	Lisa A and Huy	*Fibonacci numbers*
	Lisa T and Gabe	*Public Key Cryptography*
	Erica and Rachel	*Perfect numbers and Mersenne primes*
Thursday, December 11	Ryan and Shaun	*Mathematics and Magic*
	Nicholas and Micheal	*The Gregorian Calendar*
	Megan and Jane	*Mathematics and Music*

The final version of the written portion of your project is due the day your group does its oral presentation. You should aim for your oral presentation to be about 20 minutes long, followed by a period of 2-3 minutes for questions. Each member of the group should be involved in the presentation for approximately the same amount of time (about 10 minutes). One grade will be assigned to the entire group, so it is the responsibility of both group members to make sure that each does his or her share and understands every aspect of the project.

Each member of the class will be asked to evaluate your presentation. A copy of the evaluation sheet is included at the end of this page. Remember that attendance on the days of project presentations is **mandatory** for everyone in the class (not just the day you are presenting!)

Joy of Numbers – Project Comment Sheet

(1) Name of Project being commented upon: _____

(2) Presenters of Project being commented upon: _____

(3) Your name (optional): _____

(4) What was the most interesting thing you learned from today's presentation?

(5) What do you think the group did a good job with today?

(6) What do you think the group could have done a better job with today?

1. Divisibility in the integers

The symbol $\mathbb{Z}$ is used to denote the set of integers. This originates from the German word for number, which is *Zahl.* The set of integers is the set of all whole numbers, their negatives, and 0. In set notation, we write

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Other number systems include the natural numbers $\mathbb{N}$ (these are the positive integers), $\mathbb{N}_0$ (the natural numbers and zero), the rational numbers $\mathbb{Q}$ (all fractions of integers), the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. In this course, we are primarily interested in $\mathbb{Z}$, and occasionally $\mathbb{Q}$.

We sometimes write $a \in \mathbb{Z}$ instead of saying "a is an integer." Other notation we will sometimes use: $\forall$ means "for all" and $\exists$ means "there exists".

We recalled the commutative, associative, and distributive laws for integer arithmetic. I.e., the commutative law of addition says that $x + y = y + x$ for all integers x, y. Multiplication is also commutative. The associative law of multiplication says that $x(yz) = (xy)z$ for all integers x, y, z. Similarly, addition is associative. And the distributive law says that $x(y + z) = xy + xz$ for all $x, y, z \in \mathbb{Z}$.

What does it mean for one integer to divide another ("evenly")? Tiffany came up with the following definition:

Definition: Let $a, b \in \mathbb{Z}$. We say that a **divides** b if the fraction $\frac{b}{a}$ is an integer. Alternatively, we can say that a divides b if there exists some integer c such that $b = ac$.

Notation: We often will write $a \mid b$ for "a divides b."

Example: $2 \mid 4$ (i.e., 2 divides 6) since $6 = 2(3)$. (Using the notation in the definition, $a = 2$, $b = 6$ and $c = 3$.)

Example: $1 \mid 6$ since $6 = 1(6)$. (Here, $a = 1$, $b = 6$, and $c = 6$.)

We then bravely proved our first "theorem" (if we dare call it that!):

Theorem: Let n be any integer. Then $1 \mid n$ and $-1 \mid n$.

Proof: (class) This is clear, since for any integer n we have $n = (1)(n)$ and $n = (-1)(-n)$. □

Homework: Let a, b, and c be integers.

(1) If $a \mid b$, does $a \mid bc$?
(2) If $a \mid bc$, must $a \mid b$ or $a \mid c$?

2. More on divisibility

We began class by listing a few important axioms of the integers which we didn't mention on Tuesday. They are the *closure* axioms:

- For $x, y \in \mathbb{Z}$, $x + y \in \mathbb{Z}$ (i.e., $\mathbb{Z}$ is closed under addition).
- For $x, y \in \mathbb{Z}$, $x - y \in \mathbb{Z}$ (i.e., $\mathbb{Z}$ is closed under subtraction).
- For $x, y \in \mathbb{Z}$, $xy \in \mathbb{Z}$ (i.e., $\mathbb{Z}$ is closed under multiplication).
- $\mathbb{Z}$ is **not** closed under division (e.g, $2 \div 3 \notin \mathbb{Z}$).

We then discussed the homework. Megan answered the first question affirmatively by giving the following argument:

Theorem: Suppose a, b, and c are integers and $a \mid b$. Then $a \mid (bc)$.

Proof: (Megan) Since $a \mid b$, $\frac{b}{a} = d$ for some integer d. Multiplying by c, we see that $\frac{bc}{a} = dc$. Since d and c are integers, so is dc (closure of multiplication). Thus, a divides bc. □

I gave an alternative proof of this theorem without using fractions: Since $a \mid b$, $b = ax$ for some $x \in \mathbb{Z}$. Multiplying by c, we obtain $bc = a(xc)$. Since $xc \in \mathbb{Z}$, this equation shows that $a \mid bc$.

The second homework question was: If $a \mid bc$, must $a \mid b$ and $a \mid c$? Lisa Tran (henceforth Lisa T) gave the following counterexample: Let $a = 6$, $b = 2$ and $c = 3$. Then $a \mid bc$ (since 6 divides itself), but a does not divide b or c. Of course, there are examples of a, b, and c where it does hold, so the most we can say here is that the statement does not always hold true for all integers a, b, and c.

We introduced some more terminology: Let a and b be integers. All of the following statements mean the same thing:

- a divides b.
- a is a *factor* of b.
- a is a *divisor* of b.
- b is a *multiple* of a.

We made an important remark about zero: It is never allowed to be a divisor!! (So even $0 \mid 0$ is not allowed, even though it makes sense from the definition of divides.) So it will be implicit when we write the expression $a \mid b$ that a is non-zero. However, the expression $a \mid 0$ is allowed, and in fact holds for all non-zero integers a.

We spent the remaining time in groups trying to resolve the following questions:

(1) If $d \mid a$ and $d \mid b$ does $d \mid a + b$?
(2) If $d \mid a$ and $d \mid b$ does $d \mid a - b$?
(3) If $d \mid a$ and $d \mid b$ does $d \mid ax + by$ for all integers x and y?
(4) If $d \mid a + b$ does $d \mid a$ and $d \mid b$?
(5) If $d \mid a + b$ and $d \mid a$ does $d \mid b$?

Lisa Amen (Lisa A from now on), representing her table, answered 'yes' to Questions (1) and (2):

Theorem: Suppose $d \mid a$ and $d \mid b$. Then $d \mid a + b$ and $d \mid a - b$.

Proof: (Lisa A) As $d|\, a$, $a = dx$ for some integer x. As $d|\, b$, $a = dy$ for some $y \in \mathbb{Z}$. Adding the two equations, we get $a + b = dx + dy = d(x + y)$. Since $x + y$ is an integer, this equation says that d divides $a + b$. (Alternatively, dividing both sides by d gives $\frac{a+b}{d} = x + y \in \mathbb{Z}$.) Replacing the plus sign with a minus sign everywhere in this proof shows that $d|\, a - b$. □

Homework: Resolve Questions (3),(4), and (5) above.

3. Greatest Common Divisors

We began by discussing the homework from Monday:

Question: If $d|\, a$ and $d|\, b$, does $d|\, ax + by$ for all integers x and y?

Answer: (Ryan) The answer is 'yes'. To see this, write $a = du$ and $b = dv$ for some integers u and v. Then $ax + by = dux + dvy = d(ux + vy)$. Since $ux + vy \in \mathbb{Z}$, we see that d divides $ax + by$.

Question: If $d|\, a + b$ does $d|\, a$ and $d|\, b$?

Answer: (Gabe) The answer is 'not always'. For example, let $d = 5$, $a = 2$ and $b = 3$. Then $5|\, 2 + 3$ but 5 does not divide either 2 or 3. Of course, for some values of d, a, and b, it does hold, for example when $a = b = d$.

Question: If $d|\, a + b$ and $d|\, a$ does $d|\, b$?

Answer: (Sean) The answer is 'yes': As before, there are integers u and v such that $a + b = du$ and $a = dv$. Then $b = (a + b) - b = du - dv = d(u - v)$. Since $u - v$ is an integer, d divides b.

Our next topic is greatest common divisors.

Definition: Let a and b be integers (not both zero). A **common divisor** of a and b is an integer d which divides both a and b. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the largest common divisor of a and b.

We remarked that if d is a divisor of a nonzero number a, then $|d| \leq |a|$. This means that the set of divisors of a nonzero integer is a finite set, since there are only finitely many integers between $|a|$ and $-|a|$.

Some examples:

Example: $\gcd(4, 6) = 2$. To see this, one can list all divisors of both numbers. The divisors of 4 are -4, -2, -1, 1, 2, and 4, while the divisors of 6 are -6, -3, -2, -1, 1, 2, 3, and 6. Hence, the common divisors of 4 and 6 are -2, -1, 1, and 2, and the greatest of these is 2.

We observed the obvious fact that if d is a divisor of a then so is $-d$. Thus, we only need to list out the positive divisors of each number to find the greatest common divisor.

Example: $\gcd(7, 15) = 1$. The only divisors of 1 are 1 and -1, both of which divide 15. The greatest common divisor is therefore 1.

Example: $\gcd(-14, -21) = 7$.

We noted a couple of observations:

- If $a \neq 0$ then $\gcd(a, 0) = |a|$.
- $\gcd(a, 1) = 1$.

As the numbers get bigger, it becomes more difficult to "eyeball" the gcd of two integers. Is there a systematic procedure or method to find the gcd? One method is the brute force approach of simply finding all common divisors as illustrated above. Of course, we don't want to make an exhaustive list of all divisors of the two integers every time we want to find a gcd. (Try doing the brute force method for $a = 144$ and $b = 216$, for instance!) It turns out there is a 'fast' way to find the gcd of two numbers, even if the are quite large. We will discuss this method in our next class.

We spent much of the rest of class contemplating the following question:

Question: Let a, b be integers with $a \neq 0$. How do the integers $\gcd(a, b)$ and $\gcd(a, a + b)$ compare?

After a little experimentation with various numbers, most of the class quickly conjecture that $\gcd(a, b) = \gcd(a, a + b)$. Michael gave a proof of this:

Theorem: Let a, b be integers with $a \neq 0$. Then $\gcd(a, b) = \gcd(a, a + b)$.

Proof: (Michael) Let $d = \gcd(a, b)$ and $e = \gcd(a, a + b)$. Since $d \mid a$ and $d \mid b$ we know $d \mid a + b$. Thus, d is a common divisor of a and $a + b$. Hence, $d \leq e$. Similarly, we have $e \mid a$ and $e \mid a + b$. Then $e \mid b$ (by the Homework problem from last week). So e is a common divisor of a and b, which means $e \leq d$. Since $d \leq e$ and $e \leq d$, we must have $d = e$. □

Homework:

(1) Suppose $7 = ax + by$ where a, b, x, y are integers. What are the possible values of $\gcd(a, b)$?

(2) Suppose $a = bq + r$ where a, b, q, and r are integers, and $b \neq 0$. Prove $\gcd(a, b) = \gcd(b, r)$.

(3) Write down at least four positive and four negative numbers for each of the following sets of integers:
   - $4x$, for $x \in \mathbb{Z}$.
   - $4x + 1$, for $x \in \mathbb{Z}$.
   - $4x + 2$, for $x \in \mathbb{Z}$.
   - $4x + 3$, for $x \in \mathbb{Z}$.
   - $4x + 4$, for $x \in \mathbb{Z}$.
   - $4x - 1$, for $x \in \mathbb{Z}$.

   Make as many observations and conjectures as you can about these lists of integers.

4. The Division Theorem

We began class by discussing the third homework problem from Tuesday.

Question: What observations and conjectures can you make about the sets of integers $4x-1$, $4x$, $4x+1$, $4x+2$, $4x+3$, and $4x+4$, where x is an arbitrary integer?

The following observations were made:

- The set of integers of the form $4x$ is the same as the set of integers of the form $4x+4$.
- The set of integers of the form $4x+3$ is the same as the set of integers of the form $4x-1$.
- (Shawn) If n is an odd integer, then every integer in the sets $4x+n$ and $4x-n$ is odd.
- (Lisa A) If n is an even integer, then every integer in the sets $4x+n$ and $4x-n$ is even.
- Every integer is in one of the sets $4x$, $4x+1$, $4x+2$, and $4x+3$.
- No integer is in more than one set among $4x$, $4x+1$, $4x+2$, and $4x+3$.

We made statements similar to the last two about the sets of integers of the form $6x$, $6x+1$, $6x+2$, $6x+3$, $6x+4$, and $6x+5$. We think of x as the "quotient" of an integer upon dividing by 6, and the other number (0, 1, 2, 3, 4, or 5) as the "remainder." This brought us to the division theorem, which basically a statement that long division 'works'. The key axiom we need for the proof is that every non-empty set of nonnegative integers has a smallest element. (This is called the *Well-Ordering Axiom.*)

Theorem: (The Division Theorem) Let a, b be integers with $b > 0$. Then there exist integers q, r such that $a = bq + r$ and $0 \leq r < b$. Furthermore, for a given a there is only one integer q and one integer r such that $a = bq + r$ and $0 \leq r < b$.

Proof: Let S denote the set of all nonnegative integers of the form $a - bx$. As an example, if $a = 20$ and $b = 6$ then $S = \{2, 8, 14, 20, 26, \dots\}$. We note that S is non-empty. For, let x be any integer less than or equal to $\frac{b}{a}$. Then $bx \leq a$, so $a - bx$ is in S. By the well-ordering axiom, S must have a smallest element, call it r. As $r \in S$, $r \geq 0$. We claim that $r < b$. If not, then $r \geq b$. But then $r - b$ also in S (if $r = a - bq$ then $r - b = a - b(q + 1)$; also $r - b \geq 0$) , contradicting that r is the smallest element in S. This means that we must have $r < b$ (to avoid the contradiction). Since $r = a - bq$, $a = bq + r$ and $0 \leq r < b$.

This proves the *existence* of the integers q and r. Equally important is the *uniqueness* of q and r. That is, there are no other integers s and t such that $a = bs + t$ with $0 \leq t < b$. We didn't have time to prove this in class, but will discuss it later. □

Here are some examples:

Example: Let $a = 1150$ and $b = 12$. Then $q = 95$ and $r = 10$. That is, $1150 = 12(95) + 10$.

Example: Let $a = -28$ and $b = 6$. Then $q = -5$ and $r = 2$. That is, $-28 = 6(-5) + 2$.

We then returned to a discussion of the remaining homework problems:

Question: Suppose $7 = ax + by$ where a, b, x, y are integers. What are the possible values of $\gcd(a, b)$?

Answer: (Hui, Lisa A) Hui gave an example that $\gcd(a, b) = 1$ is posssible: namely, $a = 2$, $x = 1$, $b = 5$, $y = 1$. Then $(2)(1) + (5)(1) = 1$ and $\gcd(2, 5) = 1$. Lisa showed that 7 is also possible: $a = -7$, $x = 0$, $b = 7$, and $y = 1$. Then $(-7)(0) + (7)(1) = 7$ and $\gcd(-7, 7) = 7$. Lisa also gave a proof that 1 and 7 are the only possibilities. Let $d = \gcd(a, b)$. Then $a = du$ and $b = dv$ for some $u, v \in \mathbb{Z}$. Then $7 = ax + by = dux + dvy = d(ux + vy)$. This shows that $d \mid 7$. Since $d > 0$, we must have $d = 1$ or $d = 7$.

We state the last homework problem as a theorem, as it will be used later in the Euclidean Algorithm:

Theorem: Suppose $a = bq + r$ with $b \neq 0$. Then $\gcd(a, b) = \gcd(b, r)$.

Proof: Let $d = \gcd(a, b)$ and $e = \gcd(b, r)$. Then $a = dx$ and $b = dy$ for some integers x, y. Then $r = a - bq = dx - dyq = d(x - yq)$. This says that $d \mid r$, and thus d is a common divisor of b and r. Hence, $d \leq e$. On the other hand, we have $b = eu$ and $r = ev$ for some $u, v \in \mathbb{Z}$. Then $a = bq + r = euq + ev = e(uq + v)$, so $e \mid a$. Thus, e is a common divisor of a and b, so $e \leq d$. Hence, $e = d$. □

How might this theorem be helpful? Well, consider the problem of finding $\gcd(1150, 12)$. Dividing 12 into 1150 (using the divsion theorem), we have $1150 = (12)(95) = 10$. By the theorem, $\gcd(1150, 12) = \gcd(12, 10)$, which is easily seen to be 2. In fact, we could have repeated the process once more: $12 = (1)(10) + 2$, so the same theorem gives that $\gcd(12, 10) = \gcd(10, 2)$, which again is obviously 2. This suggests a method for calculating the gcd of any two integers, called the Euclidean Algorithm: Let a and b be positive integers. Dividing b into a we get

$$a = bq_1 + r_1$$

with $0 \leq r_1 < b$. If r_1 is not zero, we can divide r_1 into b:

$$b = r_1 q_2 + r_2$$

with $0 \leq r_2 < r_1$. If $r_2 \neq 0$, we repeat the process:

$$r_1 = r_2 q_3 + r_3$$

with $0 \leq r_3 < r_2$. Eventually, we get down to a remainder of zero:

$$r_{n-1} = r_n q_{n+1} + 0.$$

For example, consider $a = 3017$ and $b = 101$:

$$\begin{aligned} 3017 &= 101(29) + 88 \\ 101 &= 88(1) + 13 \\ 88 &= 13(6) + 10 \\ 13 &= 10(1) + 3 \\ 10 &= 3(3) + 1 \\ 3 &= 1(3) + 0 \end{aligned}$$

Homework:

(1) Why do we eventually get a remainder of 0 in the Euclidean Algorithm?
(2) Let r_n be the last nonzero remainder in the Euclidean Algorithm applied to the integers a and b. Show that $r_n = \gcd(a, b)$.

5. Linear Combinations

We recalled the Euclidean Algorithm from last class: Let a and b be two integers (assume $b \neq 0$). Dividing b into a we get

$$a = bq_1 + r_1$$

with $0 \leq r_1 < b$. If r_1 is not zero, we can divide r_1 into b:

$$b = r_1 q_2 + r_2$$

with $0 \leq r_2 < r_1$. If $r_2 \neq 0$, we repeat the process:

$$r_1 = r_2 q_3 + r_3$$

with $0 \leq r_3 < r_2$. Eventually, we get down to a remainder of zero:

$$r_{n-1} = r_n q_{n+1} + 0.$$

The first homework question was, why do we eventually get to a remainder of zero? In other words, why must the Euclidean Algorithm terminate? Megan explained that since the remainders are getting smaller and are always nonnegative, eventually we must reach a remainder of zero. In other words, since we have a sequence of nonnegative integers $b > r_1 > r_2 > r_3 > \cdots$, we must have $r_1 \leq b - 1$, $r_2 \leq b - 2$, $r_3 \leq b - 3$ so that the process must terminate in at most b steps.

The next homework problem was to explain why the last nonzero remainder in the Euclidean Algorithm is $\gcd(a, b)$. The answer is given by the theorem we proved on September 4th: If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$. Applying this to each step in the Euclidean Algorithm above, we have

$$\begin{aligned} \gcd(a, b) &= \gcd(b, r_1) \\ &= \gcd(r_1, r_2) \\ &= \gcd(r_2, r_3) \\ &\cdots \\ &\cdots \\ &= \gcd(r_n, 0) \\ &= r_n \end{aligned}$$

Example: Find $\gcd(141, 120)$:

$$\begin{aligned} 141 &= 120(1) + 21 \\ 120 &= 21(5) + 15 \\ 21 &= 15(1) + 6 \\ 15 &= 6(2) + 3 \\ 6 &= 3(2) + 0 \end{aligned}$$

This means that

$$\gcd(141, 120) = \gcd(120, 21) = \gcd(21, 15) = \gcd(15, 6) = \gcd(6, 3) = \gcd(3, 0) = 3.$$

The Euclidean Algorithm provides a fast way to compute gcds of pairs of even very large integers.

We spent the rest of class discussing "linear combinations" of integers:

Definition: Let a, b be integers. Any expression of the form $ax + by$ where $x, y \in \mathbb{Z}$ is called a **linear combination** of a and b.

Example: Let $a = 4$ and $b = 7$. Some of the linear combinations of 4 and 7 we found were:

$$\begin{aligned} 0 &= 4(0) + 7(0) \\ 4 &= 4(1) + 7(0) \\ 7 &= 4(0) + 7(1) \\ 11 &= 4(1) + 7(1) \\ 15 &= 4(2) + 7(1) \\ 1 &= 4(2) + 7(-1) \\ -3 &= 4(-2) + 7(1) \\ -4 &= 4(-1) + 7(0) \end{aligned}$$

We noted that since 1 is a linear combination of 4 and 7 then *every* integer is a linear combination of 4 and 7: Let m be an integer. Then multiplying the equation $1 = 4(2) + 7(-1)$ by m, we have $m = 4(2m) + 7(-m)$, showing that m is indeed a linear combination of 4 and 7.

We also remarked that if d is a linear combination of a and b then so is $-d$, just by multiplying the equation by -1. So from now on, we will only be interested in positive integers which are linear combinations of a and b.

We considered another example:

Example: Let $a = 8$ and $b = 12$. Some of the linear combinations of 8 and 12 we found were:

$$\begin{aligned} 8 &= 8(1) + 12(0) \\ 12 &= 8(0) + 12(1) \\ 20 &= 8(1) + 12(1) \\ 4 &= 8(-1) + 12(1) \end{aligned}$$

In this example, we wondered what the smallest positive linear combination of 8 and 12 is. Since this quantity will come up again, we made a definition:

Definition: Let a, b be integers. We define $\text{splc}(a, b)$ to be the smallest positive integer which is a linear combination of a and b.

In our first example, clearly $\text{splc}(4, 7) = 1$ since 1 is a linear combination of 4 and 7 and 1 is the smallest positive integer. In our second example, the smallest positive integer anyone could write as a linear combination of 8 and 12 was 4. Is this indeed the smallest? Or is it possible that 1, 2, or 3 is a linear combination? Hui pointed out that since $8x$ and $12y$ are even, and since the sum of two even integers is even, every linear combination of 8 and 12 must be even. Thus, $\text{splc}(8, 12)$ is either 2 or 4. Nick gave an argument that 2 is not a linear combination. For, suppose $2 = 8x + 12y$.

Dividing by 2, we get $1 = 4x + 6y$. But this says that 1 is the sum of two even numbers, which is clearly a contradiction. Hence, 2 cannot be a linear combination of 8 and 12. We can thus safely conclude that $\text{splc}(8, 12) = 4$.

At this point, Gabe was ready to make a conjecture!

Conjecture: (Gabe) Let a and b be integers (not both zero). Then $\text{splc}(a, b) = \gcd(a, b)$.

We tested this conjecture on another example:

Example: Let $a = 12$ and $b = 30$. Find $\text{splc}(12, 30)$.

Answer: We quickly noted that $6 = 12(3) + 30(-1)$, so $\text{splc}(12, 30) \leq 6$. How do we eliminate 1 through 5 as possibilities. Again, we noted that $12x$ and $30y$ are both even, so $\text{splc}(12, 3)$ must be even. However, we can eliminate all the numbers 1 through 5 simultaneously by noting that $12x + 30y = 6(2x + 5y)$, so any linear combination of 12 and 30 is a multiple of 6. Since 6 is clearly the smallest positive multiple of 6, we conclude that $\text{splc}(12, 30) \geq 6$. Thus, $\text{splc}(12, 30) = 6 = \gcd(12, 30)$.

The solution to this example suggested the following theorem.

Theorem: Let a and b be two integers (not both zero). Then any linear combination of a and b is a multiple of $\gcd(a, b)$. In particular, $\text{splc}(a, b) \geq \gcd(a, b)$.

Proof: (Michael) Let $d = \gcd(a, b)$. Then $a = dp$ and $b = dq$ for some integers p and q. Let m be a linear combination of a and b. Then $m = ax + by$ for some $x, y \in \mathbb{Z}$. Then $m = ax + by = dpx + dqy = d(px + qy)$, which shows d divides m. This proves the first statement. For the second statement, since $\text{splc}(a, b)$ is a linear combination of a and b, the first statement says that $\text{splc}(a, b)$ is a multiple of d. Since the smallest positive multiple of d is d, this shows that $\text{splc}(a, b) \geq d$.

Homework: Use the Euclidean algorithm to find the following greatest common divisors:

(1) $\gcd(7696, 4144)$
(2) $\gcd(1721, 378)$

6. The equation $ax + by = m$

We began class by going over the homework, which Jane and Erica put on the board:

Problem: Find $\gcd(1721, 378)$.

Solution: (Jane)

$$\begin{aligned} 1721 &= 378(4) + 209 \\ 378 &= 209(1) + 169 \\ 209 &= 169(1) + 40 \\ 169 &= 40(4) + 9 \\ 40 &= 9(4) + 4 \\ 9 &= 4(2) + 1 \\ 4 &= 1(4) + 0 \end{aligned}$$

This means that $\gcd(1721, 378) = 1$.

Problem: Find $\gcd(7696, 4144)$.

Solution: (Erica)

$$\begin{aligned} 7696 &= 4144(1) + 3552 \\ 4144 &= 3552(1) + 592 \\ 3552 &= 592(6) + 0 \end{aligned}$$

Thus, $\gcd(7696, 4144) = 592$.

Next, we recalled Gabe's conjecture: For integers a and b, $\gcd(a, b) = \text{splc}(a, b)$. Last time, we showed that any linear combination of a and b is a multiple of $\gcd(a, b)$. Consequently, $\text{splc}(a, b) \geq \gcd(a, b)$. To complete the proof of Gabe's conjecture, we need to show that $\gcd(a, b)$ is indeed a linear combination of a and b. Let's consider the first two steps of the Euclidean Algorithm on a and b:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \end{aligned}$$

Question: Is r_2 a linear combination of a and b?

Answer: (Erica) Yes: Solving the first equation for r_1, we have $r_1 = a - bq_1$. Substituting into the second equation, we have $r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = a(-q_2) + (1 + q_1q_2)b$. This shows that r_2 is a linear combination of a and b.

If we added the next step in the algorithm, namely $r_1 = r_2q_3 + r_3$, the Megan showed that r_3 is also a linear combination of a and b. Continuing this process, it seems plausible that every remainder in the Euclidean Algorithm is a linear combination of a and b and therefore, the $\gcd(a, b)$ (being the last nonzero remainder) is a linear combination of a and b. To make this argument more precise, we made the following definition:

Definition: Let a and b be integers. We define $\mathrm{LC}(a, b)$ to be the set of all linear combinations of a and b. In other words, $\mathrm{LC}(a, b)$ is the set of all integers $ax + by$ for some integers x and y.

So, for example, $\mathrm{LC}(6, 8) = \{\ldots, -4, -2, 0, 2, 4, 6, 8, \ldots ...\}$. In fact, one can easily show that $\mathrm{LC}(6, 8)$ is the set of all even integers. On the other hand, we've show that 1 is a linear combination of 4 and 7, and therefore all integers are linear combinations of 4 and 7. Hence, $\mathrm{LC}(4, 7) = \mathbb{Z}$.

We made a few observations of $\mathrm{LC}(a, b)$:

Theorem: Let a and b be two integers.

(1) The sum of two integers in $\mathrm{LC}(a, b)$ is in $\mathrm{LC}(a, b)$.
(2) The difference of two integers in $\mathrm{LC}(a, b)$ is in $\mathrm{LC}(a, b)$.
(3) The product of any integer with an integer in $\mathrm{LC}(a, b)$ is again in $\mathrm{LC}(a, b)$.

Proof: Lisa A gave the proof of part (a): Let m_1 and m_2 be in $\mathrm{LC}(a, b)$. Then $m_1 = ax_1 + by_1$ and $m_2 = ax_2 + by_2$ for some integers x_1, x_2, y_1, and y_2. Then $m_1 + m_2 = ax_1 + by_1 + ax_2 + by_2 = a(x_1 + x_2) + b(y_1 + y_2)$, which shows $m_1 + m_2$ is a linear combination of a and b. Hence, $m_1 + m_2 \in \mathrm{LC}(a, b)$. Gabe pointed out that the same proof shows $m_1 - m_2 \in \mathrm{LC}(a, b)$. (Just replace a couple pluses by a minuses.) And Megan proved the last part: Let m be in $\mathrm{LC}(a, b)$ and d and integer. Then $m = ax + by$ for some $x, y \in \mathbb{Z}$. So $dm = a(dx) + b(dy)$, which shows that $dm \in \mathrm{LC}(a, b)$. □

We gave a formal proof of the following:

Theorem: Let a, b be integers (not both zero). Then every remainder in the Euclidean algorithm applied to a and b is a linear combination of a and b. In particular, $\gcd(a, b)$ is a linear combination of a and b.

Proof: Consider the equations in the Euclidean algorithm:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\cdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_n + 0 \end{aligned}$$

Since $r_1 = a + b(-q_1)$, we see that r_1 in in $\mathrm{LC}(a, b)$. Suppose we have shown the first i remainders are in $\mathrm{LC}(a, b)$. At the $i + 1$st step, we have $r_{i+1} = r_{i-1} - r_iq_{i+1}$. Since r_i is in $\mathrm{LC}(a, b)$, so is r_iq_{i+1}. And since r_{i-1} is in $\mathrm{LC}(a, b)$, so is $r_{i-1} - r_iq_{i+1}$. Thus, r_{i+1} is in $\mathrm{LC}(a, b)$. This shows that every remainder in the Euclidean algorithm is in $\mathrm{LC}(a, b)$. □

As a consequence, we have completed the proof of Gabe's conjecture:

Corollary: Let a and b be integers (not both zero). Then $\mathrm{splc}(a, b) = \gcd(a, b)$.

We illustrated this procedure with an example:

Example: Using the Euclidean algorithm on 141 and 120, we get

$$\begin{aligned} 141 &= 120(1) + 21 \\ 120 &= 21(5) + 15 \\ 21 &= 15(1) + 6 \\ 15 &= 6(2) + 3 \\ 6 &= 3(2) + 0, \end{aligned}$$

so $\gcd(141, 120) = 3$. We now use "back substitution" to write each of the remainders as linear combinations of 141 and 120. Most students find it helpful to use variables (usually a and b) for 141 and 120 to keep track of the 141's and the 120's in the equations. So we start by letting $a = 141$ and $b = 120$ and substitute these letters into the first equation above. Then we find the remainder as a linear combination of a and b and substitute into the next equation in the Euclidean Algorithm. We keep doing this until we reach the gcd.

$$\begin{aligned} a = b + 21 &\implies 21 = a - b \\ b = (a - b)(5) + 15 &\implies 15 = 6b - 5a \\ a - b = (6b - 5a)(1) + 6 &\implies 6 = 6a - 7b \\ 6b - 5a = (6a - 7b)(2) + 3 &\implies 3 = 20b - 17a \end{aligned}$$

Thus, we have $3 = 141(-17) + 120(20)$. (You should always check your answer at this point.)

Next we made a very basic definition:

Definition: Let a, b, u, v, m be integers. We say that $x = u$ and $y = v$ is an (integer) **solution** to the equation $ax + by = m$ if $au + bv = m$ is a true equation. Sometimes we will say the ordered pair (u, v) is a solution to $ax + by$, where it is understood that the first coordinate is the x-value and the second coordinate is the y-value.

Example: $6(-2) + 15(1) = 3$, so $x = -2$ and $y = 1$ is a solution to $6x + 15y = 3$. Alternatively, we could say $(-2, 1)$ is a solution to $6x + 15y = 3$. We also noted that $(3, -1)$, $(-7, 3)$, and $(-12, 5)$ are also solutions. In fact, we guessed that there are infinitely many solutions to this equation.

Example: $20(-3) + 32(2) = 4$, so $(-3, 2)$ is a solution to $20x + 32y = 4$. One can see that $(5, -3)$ is also a solution to this equation.

Example: Nick showed there is there is no solution to the equation $6x + 15y = 1$, since the left-hand side is always divisible by 3 for any $x, y \in \mathbb{Z}$.

Homework:

(1) Use the Euclidean algorithm to express $\gcd(3756, 936)$ as a linear combination of 3756 and 936.
(2) Let a, b, m be integers (a and b not both zero). Make a conjecture about when the equation $ax + by = m$ has a solution (where x, y are integers).

7. A first look at primes

We started with the homework. Ryan put up the solution to the first homework problem:

Problem: Use the Euclidean algorithm to express $\gcd(3756, 936)$ as a linear combination of 3756 and 936.

Solution: (Ryan) First, we run the Euclidean algorithm to find the gcd:

$$3756 = 936(4) + 12$$
$$936 = 12(78) + 0$$

Thus, $\gcd(3756, 936) = 12$. Now we want to find x and y such that $12 = 3756x + 936y$. But this is easy, since the first line of the algorithm gives $12 = 3756(1) + 936(-4)$.

Since this was a rather trivial example, we tried another:

Problem: Express $\gcd(878, 421)$ as a linear combination of 878 and 421.

Solution: First, Hui used the Euclidean algorithm to find the gcd: First, we run the Euclidean algorithm to find the gcd:

$$878 = 421(2) + 36$$
$$421 = 36(11) + 25$$
$$36 = 25(1) + 11$$
$$25 = 11(2) + 3$$
$$11 = 3(3) + 2$$
$$3 = 2(1) + 1$$
$$2 = 1(2) + 0$$

Thus, $\gcd(878, 421) = 1$. Now we want to find x and y such that $1 = 878x + 421y$. Rachel did this part. Let $a = 878$ and $b = 421$. We now successively solve for the remainders in terms of a and b:

$$\begin{aligned}
a = b(2) + 36 &\implies 36 = a - 2b \\
b = (a - 2b)(11) + 25 &\implies 25 = 23b - 11a \\
a - 2b = (23b - 11a)(1) + 11 &\implies 11 = 12a - 25b \\
23b - 11a = (12a - 25b)(2) + 3 &\implies 9 = 73b - 35a \\
12a - 25b = (73b - 35a)(3) + 2 &\implies 2 = 117a - 244b \\
73b - 35a = (117a - 244b)(1) + 1 &\implies 1 = 317b - 152a
\end{aligned}$$

So $1 = 878(-152) + 421(317)$.

Expressed in terms of equations, our first example shows that $(1, -4)$ is a solution to $3756x + 936y = 12$, while the second example shows that $(-152, 317)$ is a solution to $878x + 421y = 1$. We then returned to the second homework problem, which asks for a conjecture about when the equation $ax + by = m$ has a solution. Erica made the first conjecture:

Conjecture: (Erica) If $\gcd(a, b)$ divides m then $ax + by = m$ has a solution.

We then, as a class, came up with a proof of this conjecture. Let $d = \gcd(a, b)$ and suppose $m = dc$ where c is an integer. We know we can find a solution (using the Euclidean algorithm) to the equation $ax + by = d$, just as in the examples above. Let's say (u, v) is a solution to $ax + by = d$; i.e., $au + bv = d$. Now multiply this equation by c to get $a(uc) + b(vc) = dc = m$. This says that (uc, vc) is a solution to $ax + by = m$!

We tried this out on the following example:

Problem: Find a solution to $141x + 120y = -18$

Solution: From our work on September 11th, we saw that $3 = \gcd(141, 120)$ and that $141(-17) + 120(20) = 3$. Multiplying this equation by -6 (to get -18 on the right-hand side), we have $141(102) + 120(-120) = -18$. This says that $(102, -120)$ is a solution to $141x + 120y = -18$.

Back to Erica's conjecture (now a theorem) and the homework problem, what can we say about $ax + by = m$ if $\gcd(a, b)$ doesn't divide m? Megan made the following conjecture:

Conjecture: (Megan) If $\gcd(a, b)$ doesn't divide m then $ax+by = m$ has no solutions.

It's helpful if we state Megan's conjecture positively: If $ax + by = m$ has a solution then $\gcd(a, b)$ must divide m. (This is called the *contrapositive* of Megan's conjecture, which is logically equivalent. So let $d = \gcd(a, b)$ and suppose $ax + by = m$ has a solution, say (u, v). Then $au + bv = m$. Now, as d divides a and b, we have $a = dp$ and $b = dq$. Then $m = dpu + pqv = d(pu + qv)$. This shows that d divides m.

Combining the two conjectures (now theorems), we have:

Theorem: The equation $ax + by = m$ has a solution if and only if $\gcd(a, b)$ divides m.

Now, suppose $ax + by = m$ has a solution. How many solutions does it have? We considered an example:

Problem: Find as many solutions as you can to the equations $6x + 15y = 3$. Can you find a pattern to the solutions?

After a few minutes, we wrote down the following solutions to the this equation: $(-2, 1)$, $(3, -1)$, $(-7, 3)$, and $(-12, 5)$. What about patterns? Shaun made the following conjecture:

Conjecture: (Shaun) For any integer c, the ordered pair $(-2+5c, 1-2c)$ is a solution to $6x + 15y = 3$.

Note that the solutions we found correspond to values of $c = 0, 1, -1$, and -2, respectively. We can check Shaun's conjecture by simply plugging the ordered pair $(-2 + 5c, 1 - 2c)$ into the equation $6x + 15y = 3$:

$$\begin{aligned} 6(-2 + 5c) + 15(1 - 2c) &= -12 + 30c + 15 - 30c \\ &= 3. \end{aligned}$$

The homework for Thursday's class was the following:

Homework:

(1) Suppose (u, v) is a solution to $ax+by = m$. Find an infinite family of solutions.
(2) Find infinitely many solutions to $577x + 366y = 27$.

On Thursday, Lisa A. and Hui proposed the following solution to the first homework problem:

Conjecture: (Lisa A. and Hui) Suppose (u, v) is a solution to $ax + by = m$ and let $d = \gcd(a, b)$. Then for any integer c, $(u+\frac{b}{d}c, v-\frac{a}{d}c)$ is also a solution to $ax+by = m$.

To prove this conjecture, all we have to do is plug in $(u+\frac{b}{d}c, v-\frac{a}{d}c)$ to the equation $ax + by = m$ and see if equality holds. Since we are given that (u, v) is a solution to $ax + by = m$, we have that $au + bv = m$. Thus,

$$\begin{aligned} a(u + \frac{b}{d}c) + b(v - \frac{a}{d}c) &= au + \frac{abc}{d} + bv - \frac{bac}{d} \\ &= au + bv \\ &= m. \end{aligned}$$

This proves Lisa and Hui's conjecture. We tried this out on the second homework problem. First, Ryan found a solution using the Euclidean algorithm:

$$\begin{aligned} 573 &= 366(1) + 207 \\ 366 &= 207(1) + 159 \\ 207 &= 159(1) + 48 \\ 159 &= 48(3) + 15 \\ 48 &= 15(3) + 3 \\ 15 &= 3(5) + 0, \end{aligned}$$

so $\gcd(573, 366) = 3$. At this point, we check to see if $3 = \gcd(573, 366)$ divides 27. It does, so we know that $573x + 366y = 27$ does have a solution. To find one, we first find a solution to $573x + 366y = 3$. Using back substitution (with $a = 573$ and $b = 366$), Ryan wrote:

$$\begin{aligned} a = b(1) + 207 &\implies 207 = a - b \\ b = (a - b)(1) + 159 &\implies 159 = 2b - a \\ a - b = (2b - a)(1) + 48 &\implies 48 = 2a - 3b \\ 2b - a = (2a - 3b)(3) + 15 &\implies 15 = 11b - 7a \\ 2a - 3b = (11b - 7a)(3) + 3 &\implies 3 = 23a - 36b. \end{aligned}$$

So $(23, -36)$ is a solution to $573x+366y = 3$. We multiply this solution by 9 to get a solution to $573x + 366y = 27$: $(207, -324)$. To find infinitely many solutions, we can

use the Lisa and Hui's theorem:

$$x = 207 + \left(\frac{366}{3}\right)c, \qquad y = -324 - \left(\frac{573}{3}\right)c$$

are solutions for any integer c. In other words, $(207 + 122c, -324 - 191c)$ gives us an infinite family of solutions to $573x + 366y = 27$.

We next returned to a question we considered during the first week of classes:

Question: Suppose $a|\, bc$ and a doesn't divide b. Must $a|\, c$?

Several people quickly gave examples showing the answer is 'not always'. For example, let $a = 6$, $b = 2$ and $c = 3$. We then considered a slight variant of the question:

Question: Suppose $a|\, bc$ and $\gcd(a, b) = 1$. Must $a|\, c$?

To investigate this question, we did several examples (one from each table) and found that in all instances the answer was 'yes.' So as a class we conjectured that the answer was always 'yes'. We then set about proving it. After awhile, Rachel came up with a proof:

Theorem: Let a, b, c be integers such that $a|\, bc$ and $\gcd(a, b) = 1$. Then $a|\, c$.

Proof: (Rachel) Since $a|\, bc$ we have $bc = ap$ for some integer p. And since $\gcd(a, b) = 1$, we have that $au + bv = 1$ for some integers u and v. Multiplying this equation by c, we have: $c = auc + bvc = auc + apv = a(uc + pv)$, which shows that $a|\, c$. □

We then made the most important definition in this course:

Definition: An integer $p > 1$ is said to be prime if its only positive divisors are 1 and p.

We listed out the first few prime numbers: 2, 3, 5, 7, 11, 13, 17, ... After a few bad jokes, we mentioned a couple open problems (among many) concerning prime numbers:

Conjecture: (The Twin Prime Conjecture) There are infinitely many pairs of integers $(p, p + 2)$ such that both p and $p + 2$ are prime.

Examples of twin primes are $(11, 13)$, $(29, 31)$, and $(41, 43)$. Another open conjecture is the following:

Conjecture: (Goldbach's Conjecture) Every even integer greater than 2 is the sum of two prime numbers.

Despite the compelling nature of these conjectures, we are not quite ready to solve them (yet!). So we returned to a more basic question.

Question: Suppose p is prime and $p|\, ab$. Must $p|\, a$ or $p|\, b$? Again, after considering a few examples, we conjecture the answer was 'yes'. To prove this, we first made the following observation:

Observation: If p is prime, then for every integer a, $\gcd(p, a) = 1$ or p. Specifically, if p divides a then $\gcd(p, a) = p$. If p does not divide a, then $\gcd(p, a) = 1$.

This observation follows immediately from the fact that p has only two (positive) divisors, 1 and p. Thus, these are the only possible values for the gcd of p and any other integer.

We then answered the previous question definitively:

Theorem: Let p be a prime and suppose $p \mid ab$. Then $p \mid a$ or $p \mid b$.

Proof: We assume that p divides ab. Now, either p divides a or it doesn't. If it does, then we're done. (We merely have to establish that p divides either a or b.) So suppose p does not divide a. By the observation, we have that $\gcd(p, a) = 1$. Thus, by Rachel's theorem above, we must have p divides b. □

There was no homework for Tuesday other than to work on the second exam.

8. More on primes

We moved onto one of the most important properties of primes: they form the "building blocks" for all the integers. First, we make a definition: An integer greater than 1 which is not prime is called *composite*.

Theorem: Every integer greater than 1 is the product of (one or more) primes.

Proof: We prove this by contradiction. That is, we assume the theorem is false and show this implies that some impossible statement must be true (the "contradiction"). The only way to avoid this "chaos" is to conclude that the statement must be true. So we start by assuming the theorem is false. This means that there must be some integer greater than 1 which is *not* the product of primes. We don't know how many such integers there are, but we know (if the theorem is false) that there must be at least one. We then let n be the smallest integer greater than 1 which is not the product of primes. (Here is the Well-Ordering Axiom at work again – see the notes from September 4th.) Now since n is not prime (else it would be the 'product' of one prime), it has a divisor d which is between 1 and n. Note that $\frac{n}{d}$, which we will label c, must also be between 1 and n. Hence, $n = dc$ where $1 < d, c < n$. Since d and c are both smaller than n and greater than 1, and n is the smallest integer greater than one which is not the product of primes, we must have that both d and c are the product of primes. But, as $n = dc$, this means that n is also the product of primes. (If $d = p_1 \cdots p_k$ and $c = q_1 \cdot \cdots \cdot q_\ell$ then $n = dc = p_1 \cdots p_k q_1 \cdots q_\ell$.) This is clearly absurd! We started with n *not* being the product of primes and we ended up with n being the product of primes. This is what we call a "contradiction". Thus, our initial assumption (that the theorem is false) must be wrong. Our conclusion, therefore, must be that the theorem is true. □

As you can see, "proof by contradiction" is a powerful tool and is used quite often in mathematics. Here is another theorem which uses contradiction in its proof:

Theorem: (Euclid, 300 BCE) There are infinitely many positive prime integers.

Proof: Suppose this statement is false. Then there must be only finitely many primes. Let's say $p_1, p_2, \ldots, p_k$ is the complete list of **all** positive primes. Now consider the integer $N = p_1 \cdot p_2 \cdots p_k + 1$. Now, Hui pointed out that N is not divisible by any prime p_i in our original list. For any prime p_i, $N = p_i q + 1$ where q is the product of the remaining primes in the list. Thus, the remainder upon dividing N by any prime p_i is one. (Here is an alternative proof: suppose p_i divides N. Then, since p_i also divides $p_1 p_2 \cdots p_n$, we have that p_i divides $N - (p_1 \cdots p_n) = 1$, which is a contradiction.) Since N is not divisible by any prime p_i then either N is a prime not in our list (contradicting our assumption) or N is not the product of primes (contradicting the theorem above). Thus, our assumption that there are only finitely many primes must be false. □

We next focused on the task of determining whether a given integer is prime or composite. Let $n > 1$ be our integer. Now, n is prime if and only if its only positive divisors are 1 and n. Thus, a simple-minded approach would be to check that no numbers between 1 and n divide n. Thus, to check if 101 is prime we would check

each number from 2 to 100 and see if it divides 101, a total of 99 calculations! Clearly, we can do better than that! Now, every integer is either prime or is divisible by a prime less than itself. Therefore, we only need to check whether any prime less than n (assuming we know what those are) divides n. That still may be a lot of calculations. For example, there are 25 primes less than or equal to 100. So to check whether 101 is prime by checking all primes less than 101, we have to do 25 calculations. Can we do better still? After doing several examples, the class came up with the following conjecture:

Conjecture: Suppose $n > 1$ is composite. Then the smallest prime divisor of n is less than or equal to $\sqrt{n}$.

The proof of this conjecture turned out to be very easy. For, suppose $n = p_1 p_2 \cdots p_k$ is a prime factorization of n and $k \geq 2$ (so that n is not prime). We assume we have written the factors so that p_1 is the smallest prime dividing n. If $p_1 > \sqrt{n}$ then $p_2 > \sqrt{n}$ also. But then $p_1 p_2 > n$, contradicting that $n = p_1 p_2 \cdots p_k$. Thus, $p_1 \leq \sqrt{n}$.

State differently (contrapositively), this proves the following primality test:

Theorem: (A simple primality test) An integer $n > 1$ is prime if and only if no prime less than or equal to $\sqrt{n}$ divides n.

As an application of this primality test, we can use this test to find a quick way of listing all the primes less than or equal to some number. In class, we did this to find all primes less than or equal to 50, but here we will list all the primes up to 120. We begin by listing all the integers from 1 to 120. We crossed off 1 because it's not prime. We know 2 is prime, but certainly any multiple of 2 can't be, so we crossed off all the even numbers greater than 2. Since 3 was the smallest number not already crossed off, we knew 3 was prime, and we crossed off all multiples of 3 (greater than 3). We did this for 5 and 7 as well. At this point, here is what the list looked like:

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100
101	102	**103**	104	105	106	**107**	108	**109**	110
111	112	**113**	114	115	116	117	118	**119**	120

Numbers in bold and underlined are not crossed off; consider everything else to be crossed off. By the simple primality test, every number less than 120 which is not prime is divisible by a prime less than $\sqrt{120}$. Since $2, 3, 5$ and 7 are the only primes less than this square root, we conclude that the numbers in bold are precisely the primes less than or equal to 120. This method is called the *Sieve of Eratosthenes* (200 BCE).

There was no homework for Thursday except to finish working on Exam # 2.

9. Mathematical Induction

We began class on a new topic: mathematical induction. The Principle of Mathematical Induction (PMI) is a way of proving a statement (such as a formula or theorem) for infinitely many integers. If we want to prove that a statement is true for all integers greater than or equal to some integer a, it suffices to prove two things:

(1) The statement is true for the integer a.
(2) Assume the statement is true for some integer $n \geq a$. Prove the statement also holds for $n+1$.

Thus an induction proof always has two parts. First one must show that the statement is true for a (to get things started). Then, assuming that the statement is true for n, one must show that it follows that the statement must also be true for $n+1$. I like to think of mathematical induction as a game of dominos (with infinitely many dominoes). The first step is to knock the first one over; the second step is to be certain (prove) that if the nth domino is knocked down then the $(n+1)$st domino will fall over as well.

Here's a more precise statement of mathematical induction. Let $P(n)$ represent some statement involving the integer n. $P(n)$ may be true or false, depending on n. Here are some examples of what $P(n)$ could be:

(1) $n^2 - n = n(n-1)$
(2) $n > n+1$
(3) $n^2 = n$
(4) $1+2+3+\cdots+n = \frac{n(n+1)}{2}$
(5) n is the product of one or more primes
(6) $2n$ is the sum of two primes

In the first example, it is clear that $P(n)$ is true for all integers n by the axioms of arithmetic. The second statement is clearly false for all integers n, while the third is true for precisely two values, 0 and 1. The fourth statement we will discuss shortly. The last two are examples of statements which don't involve formulae.

A precise statement of the Principle of Mathematical Induction (PMI) is as follows:

Theorem: (Principle of Mathematical Induction) Let $P(n)$ be a mathematical statement involving the integer n. Let a be an integer. Suppose the following two statements are true:

(1) $P(a)$ is true.
(2) If $P(n)$ is true for some $n \geq a$, then $P(n+1)$ is true.

Then $P(n)$ is true for all $n \geq a$.

Let's demonstrate PMI on an example:

Example: Prove that for all integers $n \geq 1$

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

That is, the sum of the first n integers is $\frac{n(n+1)}{2}$.

Proof: To prove this by mathematical induction, we first verify that it is true when $n = 1$. Checking, we have $1 = \frac{(1)(2)}{2}$, which is true. The next step is to assume

that the formula is true for some value n. We then need to prove the formula holds for $n+1$, i.e.,

$$1+2+\cdots+n+(n+1)=\frac{(n+1)(n+1+1)}{2}=\frac{(n+1)(n+2)}{2}.$$

We start by working with the right-hand side of this equation and use our assumption that the formula is true for the sum of the first n integers. The rest is just algebra:

$$\begin{aligned}1+2+\cdots+n+(n+1) &= \frac{n(n+1)}{2}+n+1\\ &= \frac{n(n+1)}{2}+\frac{2(n+1)}{2}\\ &= \frac{n^2+3n+2}{2}\\ &= \frac{(n+1)(n+2)}{2}.\end{aligned}$$

This shows that the formula is true for $n+1$ as well. By the Principle of Mathematical Induction, we're done! □

We then tried our hand at the following example:

Example: For all $n \geq 1$

$$1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

That is, the sum of the first n square is given by $\frac{n(n+1)(2n+1)}{6}$.

Proof: (Lisa A.) Let $P(n)$ be the formula above. Lisa first showed that $P(1)$ is true, since $\frac{(1)(1+1)(2(1)+1)}{6}=\frac{(1)(2)(3)}{6}=1=(1)^2$. The second step is to assume that $P(n)$ is true for some $n \geq 1$ and then prove that $P(n+1)$ is true. That is, we **assume** $1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$. We need to **prove** $1^2+2^2+\cdots n^2+(n+1)^2=\frac{(n+1)(n+1+1)(2(n+1)+1)}{6}=\frac{(n+1)(n+2)(2n+3)}{6}$. Starting with the left-hand side of the equation we are trying to prove and using our assumption, we have

$$\begin{aligned}1^2+2^2+\cdots+n^2+(n+1)^2 &= \frac{n(n+1)(2n+1)}{6}+(n+1)^2\\ &= (n+1)\left(\frac{n(2n+1)}{6}+\frac{6(n+1)}{6}\right)\\ &= (n+1)\left(\frac{n^2+7n+6}{6}\right)\\ &= \frac{(n+1)(n+2)(2n+3)}{6},\end{aligned}$$

which shows that the formula holds for $n+1$. By the Principle of Mathematical Induction, we have proved that $P(n)$ is true for all $n \geq 1$. □

We tried one more example, this time using a strengthening of PMI called *complete induction*. Complete induction works the same way as PMI, except that in the

induction step, when trying to prove $P(n+1)$ is true, one can assume that all $P(k)$ are true for $a \leq k \leq n$. This is sometimes necessary in order to make the argument work, as we will see in the following example:

Example: Define a function $f(n)$ for all nonnegative integers as follows:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 2 \\ f(n) &= f(n-1) + 2f(n-2), \text{ for } n \geq 2. \end{aligned}$$

We computed a few terms:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 2 \\ f(2) &= f(1) + 2f(0) = 2 + 2(1) = 4 \\ f(3) &= f(2) + 2f(1) = 4 + 2(2) = 8 \\ f(4) &= f(3) + 2f(2) = 8 + 2(4) = 16 \end{aligned}$$

At this point, several people noticed a pattern. All the terms calculated above are powers of two. So it seems reasonable to make the following conjecture: for all integers $n \geq 0$,

$$f(n) = 2^n.$$

We then gave a proof of this conjecture using complete induction:

Proof: As usual, the first step is to show that the formula is true for the base case. From our calculations above, we have already verified it for the first five values of n (including 0), so that part is done. The next step is to assume that the formula is true for all integers from 0 to n and then prove it is true for $n+1$, i.e., $f(n+1) = 2^{n+1}$. Now, since we have already verified the formula for $0 \leq n \leq 5$, we can certainly assume that $n + 1 \geq 2$. Thus, we can use the equation $f(n+1) = f(n) + 2f(n-1)$. (This is just the definition for f, but with $n+1$ substituted for n.) Now, since we know the formula is true for all integers less than or equal to n, we have that $f(n) = 2^n$ and $f(n-1) = 2^{n-1}$. Using this in combination with our definition of $f(n+1)$, we have

$$\begin{aligned} f(n+1) &= f(n) + 2f(n-1) \\ &= 2^n + 2(2^{n-1}) \\ &= 2^n + 2^n \\ &= 2(2^n) \\ &= 2^{n+1}, \end{aligned}$$

which is what we wanted to show. Thus, by (complete) induction, we have proved that $f(n) = 2^n$ for all $n \geq 0$. □

Homework:

(1) Prove that the sum of the first n odd positive integers is n^2. That is, $1 + 3 + 5 + \cdots + (2n-1) = n^2$ for all $n \geq 1$.

(2) Define a function $f(n)$ as follows: $f(0) = 1$, $f(1) = 1$, and $f(n) = f(n-1) + f(n-2)$ for $n \geq 2$. (The values of $f(n)$ form the *Fibonacci sequence*.) Prove that $f(n) \leq (\frac{7}{4})^n$ for all $n \geq 0$.

10. The E-Zone

We began class by discussing the homework. Rachel put up the answer to the first homework problem:

Example: For all $n \geq 1$

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Proof: (Rachel) For $n \geq 1$ let $P(n)$ represent the equation above. When $n = 1$, we have $1 = 1^2$, which is certainly true. Now assume $P(n)$ is true for some $n \geq 1$. That is, we assume that $1+3+5+\cdots+(2n-1) = n^2$. We need to prove the formula for is true for $n+1$. Notice that the last term on the left-hand side of the equation of $P(n+1)$ is $2(n+1)-1 = 2n+1$, which is the next odd number after $2n-1$. Adding $2n+1$ to both sides of the equation represented by $P(n)$, we get

$$\begin{aligned} 1 + 3 + \cdots + (2n - 1) + (2n + 1) &= n^2 + (2n + 1) \\ &= (n + 1)^2. \end{aligned}$$

This means that $P(n + 1)$ is true. Therefore, by PMI, we have that $P(n)$ is true for all $n \geq 1$. □

The next problem was a bit more difficult, since it involves an inequality instead of an equality. Michael got us started with the solution.

Example: Define a function $f(n)$ as follows: $f(0) = 1$, $f(1) = 1$, and $f(n) = f(n - 1) + f(n - 2)$ for $n \geq 2$. Prove that $f(n) \leq (\frac{7}{4})^n$ for all $n \geq 0$.

Proof: (Michael) For $n \geq 0$ we let $P(n)$ denote the inequality: $f(n) \leq (\frac{7}{4})^n$. We can quickly establish two base cases: $f(0) = 1 = (\frac{7}{4})^0 = 1$ (so $P(0)$ is true) and $f(1) = 1 \leq (\frac{7}{4})^1 = \frac{7}{4}$ (so $P(1)$ is true). Now we are going to use the stronger form of induction (*complete* induction): we will assume $P(0)$, $P(1)$, ...,$P(n)$ are all true and try to prove $P(n+1)$ is true. Since we established the formula for $n = 0$ and $n = 1$, we can assume $n \geq 2$. So we have $f(n+1) = f(n)+f(n-1)$. Since both $P(n)$ and $P(n-1)$ are both true (our assumption), we have that $f(n) \leq (\frac{7}{4})^n$ and $f(n-1) \leq (\frac{7}{4})^{n-1}$. This gives us that $f(n+1) = f(n)+f(n-1) \leq (\frac{7}{4})^n+(\frac{7}{4})^{n-1} = (\frac{7}{4})^{n-1}(\frac{7}{4}+1) = (\frac{7}{4})^{n-1}(\frac{11}{4})$. Now, since $\frac{11}{4} = \frac{44}{16} \leq \frac{49}{16} = (\frac{7}{4})^2$, we have

$$f(n + 1) \leq (\frac{7}{4})^{n-1}(\frac{11}{4}) \leq (\frac{7}{4})^{n-1}(\frac{7}{4})^2 = (\frac{7}{4})^{n+1}.$$

Thus, $P(n + 1)$ is true. By induction, this proves that $P(n)$ is true for all $n \geq 0$. □

We then returned to our discussion of prime numbers:

Definition: An prime number which is of the form $2^n - 1$ for some integer n is called a *Mersenne prime*.

Mersenne primes are named after the French monk Marin Mersenne (1588–1648) who studied them. One can show (and you will show on your next exam!) that if $2^n - 1$ is prime then so is n. Some Mersenne primes are:

$$3 = 2^2 - 1$$
$$7 = 2^3 - 1$$
$$31 = 2^5 - 1$$
$$127 = 2^7 - 1$$

However, Megan noted that $2^{11} - 1 = 2047$ is *not* prime, as $2047 = (23)(89)$. Thus, $2^p - 1$ is not prime for every prime integer p. It is still unknown whether there are infinitely many Mersenne primes. A research team at UCLA last week announced the discovery of a 13 million digit prime number which is the largest known prime. The prime is actually a Mersenne prime with $n = 43,112,609$.

Definition: Let $n \geq 2$ be an integer. An expression $n = p_1 \cdot p_2 \cdots p_k$ where $p_1, \ldots, p_k$ are primes is called a **prime factorization** of n.

Some examples of prime factorizations are $12 = 2 \cdot 2 \cdot 3$, $14 = 2 \cdot 7$, $100 = 2 \cdot 2 \cdot 5 \cdot 5$. We proved on September 20th that every integer greater than one has a prime factorization. We now come to an important question: Can integers have more than one prime factorization? That is, is the prime factorization of an integer *unique?* Well, clearly we could switch the order of the primes in the factorization; e.g., we could write $12 = 2 \cdot 3 \cdot 2$ instead of $2 \cdot 2 \cdot 3$. But this is not really a different factorization. Can integers have more than one prime factorization in which either the primes occurring in the factorization are different, or the number of them appearing is different? We are tempted by our experience to say that the answer is obviously "no". But how "obvious" is it? Let's make a short digression into another number system:

Consider the set of positive even integers along with one: $E = \{1, 2, 4, 6, 8, 10, \cdots\}$. Let's call this set the **E-zone**. Note that, like the integers, the E-zone is closed under multiplication. (I.e., if you multiply two positive integers, you get another positive even integer.) Let's call an E-zone integer an **E-prime** it's greater than 1 and its only E-zone factors are 1 and itself. For example, 2, 6, 10, 14, 18 are the first few E-primes. Huy made the observation that an E-zone integer is E-prime if and only if it is not divisible by 4. Another way to state it is that a number is E-prime if and only if it is twice an odd number. Moreover, the proof we did earlier can be easily adapted to show that we can factor every E-zone numbers into a product of E-primes. For example, $4 = 2 \cdot 2$, $8 = 2 \cdot 2 \cdot 2$, $12 = 2 \cdot 6$, $16 = 2 \cdot 2 \cdot 2 \cdot 2$, and $20 = 2 \cdot 10$.

Now, is the E-prime factorization of an E-zone integer unique? The class voted 'YES' overwhelmingly, but in fact that answer is 'NO', as the following example illustrates

Example: $36 = (2)(18)$ and $36 = (6)(6)$ are two different factorizations of 36 into E-primes. In the first factorization, 2 and 18 are the E-primes which occur, while in the second the E-primes are 6 and 6.

Homework:

(1) Find an E-zone integer with at least 3 different factorizations into E-primes.

(2) Let p be an E-prime and suppose p divides ab in the E-zone, where a and b are E-zone integers. (That is, $ab = px$ where x is an E-zone integer.) Must p divide a or b in the E-Zone?
(3) Find another Mersenne prime (not listed in class).

11. The Fundamental Theorem of Arithmetic

Ryan put up a solution to the first homework problem:

Example: (Ryan) 252 is E-zone number with 3 different E-prime factorizations:

$$\begin{aligned} 252 &= (2)(126) \\ &= (6)(42) \\ &= (14)(18). \end{aligned}$$

It is easily seen that 2, 126, 6, 42, 14, and 18 are E-primes since they are twice odd numbers.

In fact, we can use Ryan's example to give a solution to the second homework problem:

Example: 42 is an E-prime and divides (14)(18). However, 42 does not divide 14 or 18.

For the last homework problem, Shaun gave an example of another Mersenne prime:

Example: (Shaun) $2^{13} - 1 = 8191$ is a Mersenne prime.

We now returned to the subject of prime factorization in the integers. Recall we proved that if p is prime and p divides ab then p divides a or p divides b. (Theorem on page 16.) We will need the following strengthening of this theorem:

Proposition: Suppose p is prime and $a_1, \ldots, a_n$ are any n integers such that p divides the product $a_1 a_2 \cdots a_n$. Then p divides a_i for some i between 1 and n.

Proof: We will prove this by induction on n (the number of factors). When $n = 1$, we just have p divides a_1. Then of course p divides one of the factors (namely, a_1). In the case $n = 2$ we have that p divides $a_1 a_2$. Then by the theorem mentioned above, we know that p divides a_1 or a_2. Now let's do the induction step. Assume we know the statement is true for n factors. We need to prove the statement for $n+1$ factors. That is, if p divides $a_1 a_2 \cdots a_{n+1}$ we need to show that p divides one of the factors a_i ($i = 1, \ldots, n+1$). Group the first n factors into one number; i.e., let $c = a_1 a_2 \cdots a_n$. Then we have p divides $c a_{n+1}$. By the theorem on page 16 again, we know that p divides c or p divides a_{n+1}. If p divides a_{k+1}, we're done. If p divides $b = a_1 \cdots a_n$, we use the induction hypothesis to say that p must divide one of $a_1, \ldots, a_n$. □

We are now ready to prove one of the most important theorems about the integers:

The Fundamental Theorem of Arithmetic: Every integer greater than or equal to two has a unique factorization into prime integers. By the word *unique* we mean the following: If $n = p_1 \cdot p_2 \cdots p_k$ and $n = q_1 \cdot q_2 \cdots q_\ell$ are two prime factorizations of the integer n then $s = t$ (that is, the number of prime factors in each factorization is the same) and, after reordering, $p_1 = q_1$, $p_2 = q_2$, ..., $p_k = q_k$.

Proof: We have already proved that every integer has a prime factorization (section 12). We just need to prove the uniqueness business. To do this properly, we will prove it by induction on the number k of prime factors in the first factorization. We first do the case $k = 1$. In this case, $n = p_1$, so n is prime. Since p_1 has no other factors other than 1, it is clear that $q_1 = p_1$. And $\ell = 1$ as well (that is, the

second factorization has only one prime factor too). Now assume that the theorem is true whenever the first factorization has k prime factors. We now prove it for $k+1$ factors: Let $n = p_1 \cdots p_{k+1}$ and $n = q_1 \cdots q_\ell$. Clearly p_{k+1} (being a prime in the first factorization) divides n. Therefore, p_{k+1} divides $q_1 \cdots q_\ell$. Since p_{k+1} is prime, we know by the proposition above that p_{k+1} divides q_i for some i. After reordering the q's, we can assume p_{k+1} divides q_ℓ. Now cancel p_{k+1} and $q_{e\ll}$ from the equation $p_1 \cdots p_{k+1} = q_1 \cdots q_t$, which gives us

$$p_1 \cdots p_k = q_1 \cdots q_{\ell-1}.$$

But the first factorization now has only k prime factors. By our induction assumption, we know that the uniqueness property holds for this factorization. Thus, the number of primes appearing in the factorizations must be equal; i.e., $k = \ell - 1$. This then gives us $k+1 = \ell$, which is what we wanted. Also by induction, we know we can that $p_1 = q_1$, $p_2 = q_2$,..., $p_k = q_k$. This completes the proof! □

We moved on to a new topic: congruences.

Definition: Let a, b, and n be integers with $n > 0$. Then we say a *is congruent to* b *modulo* n if n divides $a - b$. The notation we use for this is $a \equiv b \pmod{n}$.

Here are some examples:

Example: $7 \equiv 4 \pmod{3}$ since $3 \mid (7-4)$.

Example: $12 \equiv 7 \pmod{5}$ since $5 \mid (12-7)$.

Example: $7 \equiv -3 \pmod{5}$ since $5 \mid (7-(-3))$.

We made some elementary observations:

- For any integers a and b, $a \equiv b \pmod{1}$, since 1 divides $a - b$.
- $a \equiv 0 \pmod{n}$ if and only if n divides a.
- For any integer a and $n \geq 1$, $a \equiv a \pmod{n}$.

We then proved that congruence modulo n is *symmetric*:

Theorem: Let a, b, n be integers with $n > 0$. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

Proof: Since $a \equiv b \pmod{n}$, we have $n \mid (a-b)$. Then certainly $n \mid (-1)(a-b)$, so $n \mid (b-a)$. Thus, $b \equiv a \pmod{n}$. □

Congruence modulo n is also *transitive*, as Lisa A. showed:

Theorem: Let a, b, n be integers with $n > 0$. Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $a \equiv c \pmod{n}$.

Proof: (Lisa A.) As $a \equiv b \pmod{n}$, we have $n \mid (a-b)$. This means $a - b = nx$ for some $x \in \mathbb{Z}$. Similarly, as $b \equiv c \pmod{n}$, we have $b - c = ny$ for some $y \in \mathbb{Z}$. Solving for b in each equation, we have $b = a - nx$ and $b = c + ny$. Substituting gives $a - nx = c + ny$, so $a - c = nx + ny = n(x+y)$. Hence, n divides $a - c$ and so $a \equiv c \pmod{n}$. □

Here is another proof which uses work we have done previously: We have $n|\,(a-b)$ and $n|\,(b-c)$. Therefore, n divides $(a-b)+(b-c)=a-c$. (If n divides two integers, it divides the sum of those two integers.) Consequently, $a \equiv c \pmod{n}$.

Homework: Let a, b, x, y, n be integers, with $n \geq 1$. Suppose $a \equiv b \pmod{n}$ and $x \equiv y \pmod{n}$. Must $a + x \equiv b + y \pmod{n}$?

12. More on Congruences

We began with a discussion of the homework:

Theorem: Let a, b, x, y, n be integers, with $n \geq 1$. Suppose $a \equiv b \pmod{n}$ and $x \equiv y \pmod{n}$. Then $a + x \equiv b + y \pmod{n}$.

Proof: (Huy) From the hypotheses, we have $n \mid a - b$ and $n \mid x - y$. Then $n \mid (a - b) + (x - y)$. Rewritten, this says $n \mid (a + x) - (b + y)$. Thus, $a + x \equiv b + y \pmod{n}$. □

Jane pointed out that the same result holds if addition is replaced with subtraction. That is, if $a \equiv b \pmod{n}$ and $x \equiv y \pmod{n}$ then $a - x \equiv b - y \pmod{n}$.

What happens if we multiply both sides of a congruence equation by a number? Does it the congruence still hold? Michael showed that indeed it does:

Theorem: Suppose $a \equiv b \pmod{n}$ and c is an integer. Then $ac \equiv bc \pmod{n}$.

Proof: (Michael) Since $a \equiv b \pmod{n}$, we have $n \mid a - b$. Thus, $a - b = nx$ for some $x \in \mathbb{Z}$. Multiplying by c, we have $ac - bc = nxc$, which implies $n \mid ac - bc$. Hence, $ac \equiv bc \pmod{n}$. □

Can we multiply two congruence equations, as is the case with addition and subtraction? Again, the answer is yes.

Theorem: Suppose $a \equiv b \pmod{n}$ and $x \equiv y \pmod{n}$. Then $ax \equiv by \pmod{n}$.

Proof: (Lisa A.) From the hypotheses, we have $a - b = np$ and $x - y = nm$. Rewriting, we have $a = np + b$ and $x = nm +$. Multiplying these equations together, we have $ax = (np + b)(nm + y) = npnm + npy + nmb + by = n(npm + py + mb) + by$. Then $ax - by = n(npm + py + mb)$, so $n \mid ax - by$. Thus, $ax \equiv by \pmod{n}$. □

What about taking powers of a congruence equation? This works too.

Theorem: Suppose $a \equiv b \pmod{n}$ and $m \geq 1$ is an integer. Then $a^m \equiv b^m \pmod{n}$.

Proof: (Michael, Huy) Let $P(m)$ be the statement that $a^m \equiv b^m \pmod{m}$. We will show that $P(m)$ is true for all $m \geq 1$ by induction. First, we check that $P(1)$ is true. $P(1)$ says that $a^1 \equiv b^1 \pmod{n}$, which is just our hypothesis. Next, we assume $P(m)$ is true and try to show $P(m + 1)$ is true. So we assume $a^m \equiv b^m \pmod{n}$. Multiplying this equation by $a \equiv b \pmod{n}$ gives us $a^{m+1} \equiv b^{m+1} \pmod{n}$, which is $P(m + 1)$. Hence, by induction, $P(m)$ is true for all $m \geq 1$. □

Observation: Let b and $n > 0$ be integers. What numbers a are congruent to b modulo n? Note that

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid a - b \\ &\iff a - b = nq \\ &\iff a = b + nq \end{aligned}$$

For example, if we want to write down a bunch of numbers which are congruent to 10 modulo 4, we start with 10 and add or subtract multiples of 4: So $10, 14, 18, 22$, as well as $6, 2, -2, -6$ are all congruent to 10 modulo 4.

Question: Given an integer a and a modulus n, what is the least nonnegative integer b such that $a \equiv b \pmod{n}$?

To get a handle on this question, we first did some examples:

Example: 2 is the least nonnegative integer congruent to 10 modulo 4.

Example: 5 is the least nonnegative integer congruent to 12 modulo 7.

Example: 1 is the least nonnegative integer congruent to 25 modulo 6.

At this point, we conjectured that the least nonnegative integer congruent to a modulo n is the remainder upon dividing a by n.

Theorem: The smallest nonnegative integer which is congruent to a modulo n is the remainder upon dividing a by n.

Proof: By the Division Theorem, we know there exists integers q and r such that $a = nq + r$ and $0 \leq r < n$. By definition, r is the remainder upon dividing a by n. Also, since $a - r = nq$, we see that n divides $a - r$. Thus a is congruent to r modulo n. Now let s is the smallest nonnegative integer congruent to a modulo n. Suppose $s \neq r$. Then $0 \leq s < r \leq n$, so $0 < r - s < n$. As $a \equiv r \pmod{n}$ and $a \equiv s \pmod{n}$, subtracting we get $0 \equiv r - s \pmod{n}$. Hence $n \mid r - s$. But clearly, n cannot divide an integer which is positive and less than n. Thus, s must equal r. □

We introduce some notation:

Notation: We say r is the *least nonnegative residue (lnr) of a modulo n* if r is the smallest nonnegative integer such that $r \equiv a \pmod{n}$. In this case, we write $r = a \,\%n$. By the theorem above, $a \,\%n$ is just the remainder upon dividing a by n.

13. Fast Exponentiation

Recall that $r = a\,\%m$ simply means that r is the remainder upon dividing a by m. Here are some examples:

$$\begin{aligned} 29\,\%6 &= 5 \\ -61\,\%8 &= 3 \\ 80\,\%20 &= 0 \end{aligned}$$

It is a little more difficult to find remainders for negative numbers than for positive numbers. Here's a useful trick for to remember:

Theorem: Suppose $r = a\,\%m$. If $r \neq 0$ then $m - r = -a\,\%m$. If $r = 0$ then $0 = -a\,\%m$.

The proof will be assigned as a homework exercise.

Example: Suppose we want to compute $5^{47}\,\%21$. Let's start by squaring:

$$\begin{aligned} 5^2 &= 25 \equiv 4 \pmod{21} \\ 5^4 &= (5^2)^2 \equiv 4^2 \pmod{21} \\ &\equiv 16 \pmod{21} \\ &\equiv -5 \pmod{21} \\ 5^8 &= (5^4)^2 \equiv (-5)^2 \pmod{21} \\ &\equiv 25 \pmod{21} \\ &\equiv 4 \pmod{21} \\ 5^{16} &= (5^8)^2 \equiv 4^2 \pmod{21} \\ &\equiv -5 \pmod{21} \\ 5^{32} &= (5^{16})^2 \equiv (-5)^2 \pmod{21} \\ &\equiv 4 \pmod{21} \end{aligned}$$

Now, since

$$5^{47} = 5^{32+8+4+2+1} = 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2 \cdot 5,$$

we have

$$\begin{aligned} 5^{47} &\equiv 4 \cdot 4 \cdot (-5) \cdot 4 \cdot 5 \pmod{21} \\ &\equiv 4 \cdot (-20) \cdot 20 \pmod{21} \\ &\equiv 4 \cdot 1 \cdot (-1) \pmod{21} \\ &\equiv -4 \pmod{21} \\ &\equiv 17 \pmod{21}. \end{aligned}$$

Note that even though we don't know the value of 5^{47}, we do know that $5^{47} \equiv 17 \pmod{21}$. Also notice how we used positive and negative numbers throughout the computation to keep things small and manageable. Finally, since $0 \leq 17 \leq 20$, we know that $5^{47}\,\%21 = 17$.

This method of writing an exponent as a sum of powers of two, and the calculating successive squares, is called "fast exponentiation". We tried another example:

Question: What is $7^{23}\,\%17$?

Answer: (Gabe) Begin by finding 23 as a sum of powers of 2: $23 = 16+4+2+1$. Therefore,

$$7^{23} = 7^{16+4+2+1} = 7^{16} \cdot 7^4 \cdot 7^2 \cdot 7^2.$$

Next, Gabe calculated these powers of 7 modulo 2. He did this by successive squaring:

$$\begin{aligned} 7^2 = 49 &\equiv 15 \pmod{17} \\ &\equiv -2 \pmod{17} \\ 7^4 = (7^2)^2 &\equiv (-2)^2 \pmod{17} \\ &\equiv 4 \pmod{17} \\ 7^8 = (7^4)^2 &\equiv 4^2 \pmod{17} \\ &\equiv 16 \pmod{17} \\ &\equiv -1 \pmod{17} \\ 7^{16} = (7^8)^2 &\equiv (-1)^2 \pmod{17} \\ &\equiv 1 \pmod{17} \end{aligned}$$

Therefore,

$$\begin{aligned} 7^{23} = 7^{16} \cdot 7^4 \cdot 7^2 \cdot 7^2 &\equiv 1 \cdot 4 \cdot (-2) \cdot 7 \pmod{17} \\ &\equiv 4 \cdot (-14) \pmod{17} \\ &\equiv 4 \cdot 3 \pmod{17} \\ &\equiv 12 \pmod{17}. \end{aligned}$$

Here are a few more simple examples:

Question: What is $(18)^{23}\,\%17$?

Answer: Since $18 \equiv 1 \pmod{1}7$, $(18)^{23} \equiv (1)^{23} \pmod{1}7$. Therefore, $1 = (18)^{23}\,\%17$.

Question: What is $(16)^{23}\,\%17$?

Answer: Since $16 \equiv -1 \pmod{1}7$, $(16)^{23} \equiv (-1)^{23} \pmod{1}7$. Thus, $16 = (16)^{23}\,\%17$.

We next applied our "modular arithmetic" to divisibility tests. Most everyone recalled being taught that a number is divisible by 3 if and only if the sum of its digits was divisible by 3. We want to try to prove this fact using congruences. First, we need a concrete formulation of what we mean by 'digits'.

Definition: Let n be a positive integer. We way that a string of numbers $d_k d_{k-1} \ldots d_1 d_0$ is the **base** 10 **representation for** n if $0 \le d_i \le 9$ for each i and

$$n = d_k(10)^k + d_{k-1}(10)^{k-1} + \cdots + d_1(10) + d_0.$$

Thus, the 2301 in base 10 represents the number $2\cdot(10)^3+3\cdot(10)^2+0\cdot(10)^1+1\cdot(10)^0$. With this language, we can now state the divisibility test for 3:

Theorem: Let n be a positive integer with base 10 representation $d_k d_{k-1}\dots d_0$. Then

$$n\,\%3 = (d_k + d_{k-1} + \cdots + d_1 + d_0)\,\%3.$$

In particular, 3 divides n if and only if 3 divides $d_k + d_{k-1} + \cdots + d_1 + d_0$.

Proof: First, we noticed that to say that something is divisible by 3 is the same as saying that it's congruent to 0 modulo 3. Since $10 \equiv 1 \pmod 3$, we have $10^i \equiv 1^i \equiv 1 \pmod 3$ for every positive integer i. Therefore,

$$\begin{aligned} n &= d_k(10)^k + d_{k-1}(10)^{k-1} + \cdots + d_1\cdot(10) + d_0 \\ &\equiv d_k\cdot 1 + d_{k-1}\cdot 1 + \cdots + d_1\cdot 1 + d_0 \pmod 3 \\ &\equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod 3. \end{aligned}$$

Therefore, $n \equiv 0 \pmod 3$ if and only if $(d_k + \cdots + d_0) \equiv 0 \pmod 3$. □

Since $10 \equiv 1 \pmod 9$, the same proof gives us a divisibility test for 9:

Theorem: Let n be a positive integer with base 10 representation $d_k d_{k-1}\dots d_0$. Then

$$n\,\%9 = (d_k + d_{k-1} + \cdots + d_1 + d_0)\,\%9.$$

In particular, 9 divides n if and only if 9 divides $d_k + d_{k-1} + \cdots + d_1 + d_0$.

Finally, here is a divisibility test for 4:

Theorem: Let n be a positive integer with base 10 representation $d_k\dots d_0$. Then $n \equiv 10d_1 + d_0 \pmod 4$. In particular, n is divisible by 4 if and only if $10d_1 + d_0$ is divisible by 4.

Proof: First, note that $100 \equiv 0 \pmod 4$. Hence, $(10)^j \equiv 0 \pmod 4$ for all $j \geq 2$. Thus, for any integer n

$$\begin{aligned} n &= d_k(10)^k + d_{k-1}(10)^{k-2} + \cdots + d_1\cdot(10) + d_0 \\ &\equiv d_k\cdot 0 + d_{k-1}\cdot 0 + \cdots + d_2\cdot 0 + d_1\cdot 10 + d_0 \pmod 4 \\ &\equiv 10d_1 + d_0 \pmod 4. \end{aligned}$$

In particular, $n \equiv 0 \pmod 4$ if and only if $10d_1 + d_0 \equiv 0 \pmod 4$.

Homework:

(1) Compute the last 2 digits of 23^{23}.
(2) Find a divisibility test for 11.

14. More on Exponentiation

We began with a discussion of the homework:

Example: Find the last two digits of 23^{23}.

Answer: The crucial observation is that the last two digits of any number are precisely the remainder you get when you divide that number by 100. Thus, we just need to find $23^{23}\,\%100$. Rachel started by finding successive squares of 23 modulo 100.

$$\begin{aligned} 23^2 = 529 &\equiv 29 \pmod{100} \\ 23^4 = (23^2)^2 &\equiv 29^2 \pmod{100} \\ &\equiv 841 \pmod{100} \\ &\equiv 41 \pmod{100} \\ 23^8 = (23^4)^2 &\equiv 41^2 \pmod{100} \\ &\equiv 1681 \pmod{100} \\ &\equiv 81 \pmod{100} \\ 23^{16} = (23^8)^2 &\equiv (81)^2 \pmod{100} \\ &\equiv 61 \pmod{100} \end{aligned}$$

Therefore,

$$\begin{aligned} 23^{23} = 23^{16+4+2+1} = 23^{16} \cdot 23^4 \cdot 23^2 \cdot 23^1 &\equiv (61 \cdot 41) \cdot (29 \cdot 23) \pmod{100} \\ &\equiv 2501 \cdot 667 \pmod{100} \\ &\equiv 1 \cdot 67 \pmod{100} \\ &\equiv 67 \pmod{100}. \end{aligned}$$

So the last two digits of 23^{23} are 6 and 7. □

We then tried another problem of this type:

Example: Find $(923)^{33}\,\%15$.

First, we find the lnr of 923 modulo 15, which is 8. That is,

$$923 \equiv 8 \pmod{1)5}.$$

Next, we begin finding successive squares of 8 modulo 15:

$$\begin{aligned} 8^2 = 64 &\equiv 4 \pmod{15} \\ 8^4 = (8^2)^2 &\equiv 4^2 \pmod{15} \\ &\equiv 1 \pmod{15} \\ 8^8 = (8^4)^2 &\equiv 1^2 \pmod{15} \\ &\equiv 1 \pmod{15} \\ 8^{16} = (8^8)^2 &\equiv 1^2 \pmod{15} \\ &\equiv 1 \pmod{15} \\ 8^{32} = (8^{16})^2 &\equiv 1^2 \pmod{15} \\ &\equiv 1 \pmod{15} \end{aligned}$$

Therefore,

$$\begin{aligned} 8^{33} = 8^{32+1} = 8^{32} \cdot 8^1 &\equiv (1)(8) \pmod{15} \\ &\equiv 8 \pmod{15}. \end{aligned}$$

Thus, $(923)^{33} \equiv 8 \pmod{15}$, and so $8 = (923)^{33} \%15$.

Next, we found a divisibility test for 11. The key observation is that $10 \equiv -1 \pmod{11}$:

Theorem: Let n be a positive integer with base 10 representation $d_k d_{k-1} \ldots d_0$. Then

$$n \%11 = (d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k) \%11.$$

In particular, 11 divides n if and only if 11 divides $d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k$.

Proof: Note that $10 \equiv -1 \pmod{11}$. Thus

$$\begin{aligned} n &= d_k(10)^k + d_{k-1}(10)^{k-1} + \cdots + d_1 \cdot (10) + d_0 \\ &\equiv d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \cdots - d_1 \cdot 1 + d_0 \pmod{11} \\ &\equiv (-1)^k d_k + (-1)^{k-1} d_{k-1} + \cdots - d_1 + d_0 \pmod{11}. \end{aligned}$$

□

We next investigated the following question:

Question: Suppose a, b, m are integers, with $m > 0$, and suppose $ab \equiv 0 \pmod{m}$. Must $a \equiv 0 \pmod{m}$ or $b \equiv 0 \pmod{m}$?

To get a handle on this question, we made several tables where we did all possible multiplications modulo m, where $m = 3, 4, 5, 6, 7$. Note that every integer is congruent to an integer in the range $0, 1, ..., m-1$. Since zero times any integer is zero, in the tables below we look at all possible products of integers between 1 and $m-1$:

Multiplication Modulo 3

	1	2
1	1	2
2	2	1

Multiplication Modulo 4

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Multiplication Modulo 5

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Multiplication Modulo 6

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Multiplication Modulo 7

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Essentially, to answer the question above we are looking for moduli which have a zero in the table somewhere, since this will correspond to two integers which are nonzero modulo m but whose product is zero modulo m. For instance, when $m = 4$, we see a zero in the table which corresponds to the fact that $2 \cdot 2 \equiv 0 \pmod 4$. Similarly, in the $m = 6$ table, we see zeros corresponding to $2 \cdot 3 \equiv 0 \pmod 6$ and $3 \cdot 4 \equiv 0 \pmod 6$. On the other hand, the multiplication tables for $m = 3, 5$, and 7 have no zeros in them. This led Gabe to make the following conjecture:

Conjecture: (Gabe) Suppose $p > 0$ is prime and a, b are two integers. If $ab \equiv 0 \pmod p$ then $a \equiv 0 \pmod p$ or $b \equiv 0 \pmod p$.

The homework for next Thursday is:

Homework:

(1) Prove Gabe's conjecture.
(2) Suppose $r = a \,\%m$ and $r > 0$. Prove $m - r = -a \,\%m$.

15. Cancellation modulo m

We began by discussing the homework.

Theorem: Suppose $r = a\,\%m$ and $r > 0$. Then $m - r = -a\,\%m$.

Proof: (Lisa A) Since $r = a\,\%m$, this means that r is the remainder upon dividing a by m. That is, $a = mq + r$ where $0 \leq r \leq m - 1$. Multiplying this equation by -1 gives:

$$\begin{aligned} -a &= m(-q) - r \\ &= m(-q) - m + m - r \\ &= m(-q - 1) + (m - r). \end{aligned}$$

Since our hypothesis is that $r > 0$, we have $1 \leq r \leq m - 1$. Multiplying by -1 and adding m, we have $1 \leq m - r \leq m - 1$. This means that $m - r$ is the remainder upon dividing $-a$ by m. Thus, $m - r = -a\,\%m$. □

Next, we proved Gabe's conjecture:

Theorem: Let p be a prime and suppose $ab \equiv 0 \pmod{p}$. Then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Proof: (Rachel) Suppose $ab \equiv 0 \pmod{p}$. Then $p \mid ab$. By a previous theorem (proved on September 18), since p is prime we have $p \mid a$ or $p \mid b$. Thus, $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. □

As a consequence, we get the following 'cancellation theorem':

Theorem: Let p be a prime and a, b, c integers. Suppose $ab \equiv ac \pmod{p}$ and $a \not\equiv 0 \pmod{p}$. Then $b \equiv c \pmod{p}$.

Proof: Subtracting, we get $a(b - c) \equiv 0 \pmod{p}$. By the theorem we just proved, either $a \equiv 0 \pmod{p}$ or $b - c \equiv 0 \pmod{p}$. Since $a \not\equiv 0 \pmod{p}$, we must have $b - c \equiv 0 \pmod{p}$; thus, $b \equiv c \pmod{p}$. □

More on cancellation when the modulus is not prime will be investigated on your take-home exam. Next, we investigated the following question:

Question: Given a modulus $m > 0$ and an integer a such that $1 \leq a \leq m - 1$, will there always be a positive k such that $a^k \equiv 1 \pmod{m}$? If there isn't always such a k, under what conditions will there will be one?

To answer this question it would first help if we looked at several examples in a systematic way. For instance, let's analyze all cases for the modulus $m = 3$. In this case, we only need to consider $a = 0$, $a = 1$ and $a = 2$, since every integer is congruent to either 0, 1, or 2 modulo 3 (these are the only possible remainders). Of course, if $a = 0$ then there is no k such that $0^k \equiv 1 \pmod{3}$. If $a = 1$ then certainly $k = 1$ works. If $a = 2$ then we easily see that $k = 2$ works. In the same way, we also investigated all possible values of a for moduli up to 8. The information we gathered is contained in the following table:

m	list of all a with $1 \leq a \leq m-1$ and $a^k \equiv 1 \pmod{m}$ for some positive k (the smallest such k is in parenthesis)
2	1 ($k=1$)
3	1 ($k=1$), 2 ($k=2$)
4	1 ($k=1$), 3 ($k=2$)
5	1 ($k=1$), 2 ($k=4$), 3 ($k=4$), 4 ($k=2$)
6	1 ($k=1$), 5 ($k=2$)
7	1 ($k=1$), 2 ($k=3$), 3 ($k=6$), 4 ($k=3$), 5 ($k=6$), 6 ($k=2$)
8	1 ($k=1$), 3 ($k=2$), 5 ($k=2$), 7 ($k=2$)

At this point, we looked for patterns. In particular, we wanted to see if there was a pattern to the numbers in each row. Huy noticed that the values of a such that there exists a $k > 0$ with $a^k \equiv 1 \pmod{m}$ all have greatest common divisor 1 with m:

Conjecture: (Huy) Let $m > 0$ and a an integer between 1 and $m-1$. Then there exists a positive integer k such that $a^k \equiv 1 \pmod{m}$ if and only if $\gcd(a, m) = 1$.

Using our cancellation theorem, we were able to prove Huy's conjecture in the case m is prime.

Theorem: Let p be prime and suppose $a \not\equiv 0 \pmod{p}$. Then there is an integer $k > 0$ such that $a^k \equiv 1 \pmod{p}$.

Proof: Since there are only p possible values for a remainder when dividing by p, among all powers a^k, $k = 1, 2, 3, \ldots$ there must be at least two such powers which give the same remainder. Say a^s and a^t give the same remainder upon dividing by p, where $0 < s < t$. Then $a^s \equiv a^t \pmod{p}$. Rewriting, we have $aa^{s-1} \equiv aa^{t-1} \pmod{p}$. Since $a \not\equiv 0 \pmod{p}$, by the cancellation theorem we have $a^{s-1} \equiv a^{t-1} \pmod{p}$. Continuing to cancel a's from both sides, we eventually get $1 \equiv a^{t-s} \pmod{p}$. Since $t - s > 0$, the theorem is proved. □

No homework was assigned for Tuesday, except to work on the exam.

16. Powers modulo m

We began the day's discussion with the following observation:

Observation: (Michael) Let a, b be integers and $m > 0$. Suppose $a^k \equiv 1 \pmod{m}$ and $b^\ell \equiv 1 \pmod{m}$ for some positive integers k and ℓ. Then $a^n \equiv 1 \pmod{m}$ and $b^n \equiv 1 \pmod{m}$ where $n = k\ell$.

Proof: Since $a^n = a^{k\ell} = (a^k)^\ell$, we have

$$\begin{aligned} a^n &\equiv (a^k)^\ell \pmod{m} \\ &\equiv (1)^\ell \pmod{m} \\ &\equiv 1 \pmod{m}. \end{aligned}$$

In the same way, $b^n \equiv 1 \pmod{m}$ as well. □

Megan noted that this argument can be generalized to more than two elements: if $a_1^{k_1} \equiv 1 \pmod{m}$, $a_2^{k_2} \equiv 1 \pmod{m}, \ldots,$ $a_r^{k_r} \equiv 1 \pmod{m}$, then for all i between 1 and r we have $a_i^n \equiv 1 \pmod{m}$ where $n = k_1 k_2 \cdots k_r$. That is, if for each i there is a positive power of a_i which is congruent to 1 modulo m then there is a *single* positive integer n such that a_i^n is congruent to 1 modulo m for *all* a_i (namely, the product of all the exponents). However, it is likely that the product of all the exponents is not the smallest common exponent which works for all i.

Recall we proved last Thursday that if p is prime and a is between 1 and $p-1$ then there is a positive integer k such that $a^k \equiv 1 \pmod{p}$. By the argument in the above paragraph, there is a single exponent k such that $a^k \equiv 1 \pmod{p}$ for *all* a between 1 and $p-1$. This led us to the following question:

Question: Given a prime p, what is the smallest positive integer k such that $a^k \equiv 1 \pmod{p}$ for all $a \not\equiv 0 \pmod{p}$?

To try to get a handle on this question, we looked at the first few primes and, using the tables we produced on October 23, we found the smallest exponent which works:

value of p:	2	3	5	7	11
smallest k:	1	2	4	6	10

This led Huy to make the following conjecture:

Conjecture: (Huy) Let p be a prime. Then $p-1$ works for all a not divisible by p. That is, $a^{p-1} \equiv 1 \pmod{p}$ for all $1 \le a \le p-1$.

No homework was assigned for Thursday (except to finish the exam).

17. Fermat's Theorem

We spent the first part of class going over the exam. In the process, we proved the following theorem, which was conjectured by Ryan:

Theorem: (Cancellation Theorem, Version II) Suppose $ab \equiv ac \pmod{m}$ and $\gcd(a, m) = 1$. Then $b \equiv c \pmod{m}$.

Proof: Since $ab \equiv ac \pmod{m}$, we have that $m \mid (ab - ac)$; i.e., $m \mid a(b - c)$. Since $\gcd(a, m) = 1$, we have by the Theorem on page 17 that $m \mid b - c$. Thus, $b \equiv c \pmod{m}$. □

We then moved on to proving Huy's conjecture from last time. Recall that Huy conjectured that if p is prime and $1 \leq a \leq p - 1$, then $a^{p-1} \equiv 1 \pmod{p}$. Of course, since every integer which is not divisible by p is congruent to an integer a between 1 and $p - 1$, we could rephrase Huy's conjecture as follows: If $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$. However, if we multiply both sides of this equation by a, we get $a^p \equiv a \pmod{p}$, which also holds even if $a \equiv 0 \pmod{p}$. This is the result we will prove, which is called *Fermat's Theorem*. This is the same Fermat of Fermat's Last Theorem fame, so some people prefer to call this Fermat's *Little* Theorem to distinguish it from his "big" theorem (which he probably never proved).

Theorem: (Fermat's Theorem) Let p be a prime. Then $a^p \equiv a \pmod{p}$ for all integers a.

Proof: We first prove this for all integers $a \geq 0$ using induction. The base case is when $a = 0$, which is certainly true, since $0^p \equiv 0 \pmod{p}$. Suppose now that $a \geq 0$ and we know that $a^p \equiv a \pmod{p}$. We need to prove that the equation is true for $a + 1$, i.e., $(a + 1)^p \equiv a + 1 \pmod{p}$. Using the result of one of the problems from Test # 4, Michael showed that:

$$\begin{aligned}(a+1)^p &\equiv a^p + 1^p \pmod{p} \\ &\equiv a^p + 1 \pmod{p} \\ &\equiv a + 1 \pmod{p} \qquad (\text{since } a^p \equiv a \pmod{p}).\end{aligned}$$

Hence, $(a + 1)^p \equiv a + 1 \pmod{p}$. Thus, we know the theorem is true for all $a \geq 0$. Now suppose $a < 0$. Then $-a > 0$. By the case above, we know that $(-a)^p \equiv -a \pmod{p}$. But $(-a)^p = (-1)^p a^p$. If p is odd, $(-1)^p = -1$ and our equation becomes $(-1)a^p = -a \pmod{p}$. Multiplying both sides of this equation by -1, we get $a^p \equiv a \pmod{p}$, which is what we wanted to show. If $p = 2$, we note that $-1 \equiv 1 \pmod{p}$ and so our equation once again becomes $a^p \equiv a \pmod{p}$. □

As an immediate corollary, we obtain a proof of Huy's conjecture:

Corollary: Let p be a prime and suppose p does not divide a. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: We have by Fermat's theorem that $a^p \equiv a \pmod{p}$. If p does not divide a then $a \not\equiv 0 \pmod{p}$. Since p is prime, we can cancel an a from both sides of the equation (by the Cancellation Theorem), obtaining $a^{p-1} \equiv 1 \pmod{p}$. □

Here is an example of how the above corollary (also sometimes called Fermat's Theorem) can be applied:

Example: Find $8^{442}\,\%23$.

First note that, by Fermat's Theorem, $8^{22} \equiv 1 \pmod{23}$. Since $442 = (22)(20)+2$, we have

$$\begin{aligned} 8^{442} = (8^{22})^{20} \cdot 8^2 &\equiv (1)^{20}(64) \pmod{23} \\ &\equiv 18 \pmod{23} \end{aligned}$$

Here is your homework for Tuesday:

Homework:

(1) Let a, b, c be integers and suppose $a|\, c$ and $b|\, c$. Suppose $\gcd(a, b) = 1$. Prove that $ab|\, c$.
(2) Find $3^{31063}\,\%17$.

18. More on Fermat's Theorem and inverses modulo m

We began with the homework which was assigned last Thursday:

Example: Find $3^{31063}\,\%17$.

Answer: By Fermat's theorem, we have that $3^{16} \equiv 1 \pmod{17}$. Dividing 16 into 31063, we have $31063 = (1941)(16) + 7$. Hence

$$\begin{aligned} 3^{31063} &= 3^{(1941)(16)+7} \\ &= (3^{16})^{1941} \cdot 3^7 \\ &\equiv (1)^{1941} \cdot 3^7 \pmod{17} \\ &\equiv 3^7 \pmod{17} \\ &\equiv 3^4 \cdot 3^3 \pmod{17} \\ &\equiv 81 \cdot 27 \pmod{17} \\ &\equiv 13 \cdot 10 \pmod{17} \\ &\equiv 11 \pmod{17} \end{aligned}$$

Since we will need the result of the second homework problem later, we state it as a theorem:

Theorem: Let a, b, c be integers and suppose $a|\,c$ and $b|\,c$. Suppose $\gcd(a, b) = 1$. Then $ab|\,c$.

Proof: (Erica) We have $c = ad$ and $c = be$ for some integers d and e. Since $\gcd(a, b) = 1$, we have that $1 = ax + by$. Multiplying by c, we obtain $c = axc + byc = axbe + byad = ab(xe + yd)$. Thus, ab divides c. □

We then moved on to a discussion of a new proof of Fermat's Theorem.

First we introduce some notation. Let p be a prime. Let

$$S_p = \{1, 2, 3, \ldots, p - 1\}.$$

That is, S_p is the set of all the numbers between 1 and $p - 1$. Given $a, b \in S_p$, note that $ab\%p$ is also in S_p. If not, then $ab\,\%p = 0$, which means p divides ab. As p is prime, this would mean that p divides a or p divides b, contradicting that a and b are between 1 and $p - 1$. For $a \in S_p$ define a function $f : S_p \to S_p$ by $f_p^a(i) = ai\,\%p$ for each $i \in S_p$.

$$aS_p = \{a\,\%p, 2a\,\%p, \ldots, (p - 1)a\,\%p\}.$$

Let's do an example with $p = 5$. We have $S_5 = \{1, 2, 3, 4\}$. Choose a random element in S_5, say 3. Then

$$\begin{aligned} f_5^3(1) &= 3 \cdot 1\,\%5 = 3 \\ f_5^3(2) &= 3 \cdot 2\,\%5 = 1 \\ f_5^3(3) &= 3 \cdot 3\,\%5 = 4 \\ f_5^3(4) &= 3 \cdot 4\,\%5 = 5 \end{aligned}$$

Notice that every element in S_5 was 'hit'; that is, the map is *onto*. We tried another example: say, $p = 7$ and $5 \in S_7$. We have

$$\begin{aligned} f_7^5(1) &= 5 \cdot 1 \,\%7 = 5 \\ f_7^5(2) &= 5 \cdot 2 \,\%7 = 3 \\ f_7^5(3) &= 5 \cdot 3 \,\%7 = 1 \\ f_7^5(4) &= 5 \cdot 4 \,\%7 = 6 \\ f_7^5(3) &= 5 \cdot 5 \,\%7 = 4 \\ f_7^5(4) &= 5 \cdot 6 \,\%7 = 2 \end{aligned}$$

Again, we see that f_7^5 is onto.

Megan made the following conjecture:

Conjecture: Suppose p is prime and $a \in S_p$. Then the map $f_p^a : S_p \to S_p$ is onto.

To help prove this conjecture, we made the following observation:

Observation: Let $f : S \to T$ be a function and suppose S and T have the same number of elements. If f is one-to-one then f is onto.

This observation follows from the *Pigeonhole Principle*, which says that if you have $n + 1$ pigeons to put into n holes, at least two pigeons have to go into the same hole. To see how this applies to the function $f : S \to T$, let's say that both S and T have n elements. If f is not onto, then the elements of S are being mapped by f into a subset of T consisting of at most $n - 1$ elements. Thus, at least two elements of S must be mapped to the same element, contradicting that f is one-to-one.

Now let's prove Megan's conjecture:

Theorem: Let p be prime and $a \in S_p$. Then $f_p^a : S_p \to S_p$ is onto.

Proof: By the observation, it suffices to prove that f_p^a is one-to-one. Suppose $f_p^a(i) = f_p^a(j)$ for some elements $i \neq j$ in S_p. Then $ai \,\%p = aj \,\%p$, which means $ai \equiv aj \pmod{p}$. Since $a \not\equiv 0 \pmod{p}$, by cancellation we have that $i \equiv j \pmod{p}$. But, since i and j are between 1 and $p - 1$, this means that $i = j$, a contradiction. Hence, f_p^a must be one-to-one (and thus onto). □

We now are in a position to use Megan's conjecture to give another proof of Fermat's Theorem:

Theorem: Let p be a prime and a an integer such that $a \not\equiv 0 \pmod{p}$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: It is enough to prove this in the case $a \in S_p$, since every integer not divisible by p is congruent to it's remainder upon dividing by p. By Megan's conjecture,

$f_p^a : S_p \to S_p$ is one-to-one and onto, we have

$$\begin{aligned} S_p &= \{1, 2, \ldots, p-1\} \\ &= \{f_p^a(1), f_p^a(2), \ldots, f_p^a(p-1)\} \\ &= \{a \,\%p, 2a \,\%p, \ldots, (p-1)a \,\%p\} \end{aligned}$$

Since the elements in these sets are the same (with just the order scrambled), we get the following products are equal:

$$1 \cdot 2 \cdot \cdots \cdot (p-1) = (a \,\%p) \cdot (2a \,\%p) \cdots ((p-1)a \,\%p).$$

Going modulo p, we have

$$(p-1) \equiv (p-1)a^{p-1} \pmod{p}.$$

But since p is prime, p does not divide $(p-1)$, so $(p-1) \not\equiv 0 \pmod{p}$. By cancellation, we then have

$$1 \equiv a^{p-1} \pmod{p}.$$

□

We now make the following definition:

Definition: Let p be prime and a an integer not divisible by p. The **order of** a **modulo** p, denoted by $o_p(a)$, is defined to be the smallest positive integer k such that $a^k \equiv 1 \pmod{p}$.

By definition, $o_p(a) \geq 1$ for all $a \not\equiv 0 \pmod{p}$. By Fermat's Theorem, we also have $o_p(a) \leq p-1$. However, it is possible for $o_p(a)$ to be less than $p-1$. For instance, $o_p(1) = 1$ no matter what p is. Here are some more examples:

Example: $o_7(2) = 3$, since $2^3 = 8 \equiv 1 \pmod{7}$ and $2^k \not\equiv 1 \pmod{7}$ for $k = 1, 2$.

Example: $o_5(3) = 4$, since $3^4 = 81 \equiv 1 \pmod{5}$ and $3^k \not\equiv 1 \pmod{5}$ for $k = 1, 2, 3$.

Here is your homework for Thursday:

Homework:

(1) Find $o_7(a)$ for $1 \leq a \leq 6$.
(2) Prove $o_p(p-1) = 2$ if p is an odd prime.
(3) Prove that $o_p(a) \,|\, p-1$ for all $1 \leq a \leq p-1$

On Thursday, we began by doing these homework problems:

Example: Find $o_7(a)$ for $1 \leq a \leq 6$.
The values are given in the following table:

a:	1	2	3	4	5	6
$o_7(a)$:	1	3	6	3	6	2

For the second homework problem, we noted that $p - 1 \equiv -1 \pmod{p}$. Hence,

$$\begin{aligned} (p-1)^2 &\equiv (-1)^2 \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

This says that $o_p(p-1) \leq 2$. But if $o_(p-1) = 1$ then $p - 1 \equiv 1 \pmod{p}$, which means $p = 2$, contradicting that p is odd.

Theorem: Let p be a prime and $a \not\equiv 0 \pmod{p}$. Then $o_p(a) | \, p-1$.

Proof: Let $n = o_p(a)$. By the division theorem, we have that $p-1 = nq+r$ where $0 \leq r \leq n-1$. We want to show $r = 0$. Suppose $r > 0$. Then since $a^n \equiv 1 \pmod{p}$ (by the definition of $o_p(a)$ and $a^{p-1} \equiv 1 \pmod{p}$ (by Fermat), we have

$$\begin{aligned} 1 &\equiv a^{p-1} \pmod{p} \\ &\equiv a^{nq+r} \pmod{p} \\ &\equiv (a^n)^q \cdot a^r \pmod{p} \\ &\equiv (1)^q \cdot a^r \pmod{p} \\ &\equiv a^r \pmod{p} \end{aligned}$$

But this says that $a^r \equiv 1 \pmod{p}$ and $1 \leq r \leq n-1$. But $n = o_p(a)$, so n is the smallest positive integer such that $a^n \equiv 1 \pmod{p}$. To avoid this contradiction, we must have $r = 0$. Hence, $p - 1 = nq$ and so $n | \, p-1$. □

Next, we changed subjects and talked about multiplicative inverses. Recall that in the usual real number arithmetic to divide by a nonzero number a is the same as multiplying by $\frac{1}{a}$ or a^{-1}. The important property of a^{-1} is that $a^{-1} \cdot a = 1$. For example, to solve an equation of the form $ax = b$, we just multiply both sides by a^{-1} to find the solution:

$$\begin{aligned} ax &= b \\ a^{-1}(ax) &= a^{-1}b \\ (a^{-1}a)x &= a^{-1}b \\ 1 \cdot x &= a^{-1}b \\ x &= a^{-1}b. \end{aligned}$$

The mathematical term for a^{-1} is the *multiplicative inverse*, or simply *inverse*, of a.

This leads to the question of whether inverses exist in the "modular world." We made the following definition:

Definition: Let a and m be integers with $m > 1$. We say that an integer b is an *inverse* for a modulo m if $ba \equiv 1 \pmod{m}$. In this case, we write $b \equiv a^{-1} \pmod{m}$.

Example: Note that 2 is an inverse for 6 modulo 11 since $2 \cdot 6 \equiv 1 \pmod{11}$.

Example: Note that 6 does not have an inverse modulo 4, since $6k \not\equiv 1 \pmod{4}$ for $k = 0, 1, 2, 3$.

This brings up the obvious question:

Question: When does an integer a have an inverse modulo m?

To answer this question, we looked at our multiplication tables modulo m for $m = 3, 4, 5, 6, 7, 8, 9$. The multiplication tables for $1 \leq m \leq 7$ were listed on October 16th. Here are the tables for $m = 8$ and $m = 9$ (which we did in class):

Multiplication Modulo 8

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Multiplication Modulo 9

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

An element has an inverse if and only if there is a 1 which appears in its row. For example, in the modulo 8 table, we see that $1, 3, 5, 7$ have inverses, but $2, 4, 6$ (and obviously 0) do not. Similarly, in the $m = 9$ table, we have $1, 2, 4, 5, 7, 8$ have inverses while 3 and 6 do not. Based on this evidence (together with the evidence from the other tables), Lisa made the following conjecture:

Conjecture: (Lisa) Let a, m be integers with $m \geq 2$. Then a has an inverse modulo m if and only if $\gcd(a, m) = 1$

And actually, Lisa was able to come up with a proof of one direction of this conjecture:

Theorem: Let a and m be integers, with $m \geq 2$. Suppose $\gcd(a, m) = 1$. Then a has an inverse modulo m.

Proof: (Lisa) Since $\gcd(a, m) = 1$ we have $ax + my = 1$ for some integers x and y. Then $my = ax - 1$ so $m \mid (ax - 1)$. Hence, $ax \equiv 1 \pmod{m}$, which means x is an inverse for a modulo m. □

In fact, Lisa's proof suggests a method for finding the inverse of a modulo m if $\gcd(a, m) = 1$. First, use the Euclidean Algorithm to find integers x and y such that $ax + my = 1$. Then the proof above shows that x is an inverse for a modulo m.

Question: What is $(13)^{-1} \pmod{1000}$?

Answer: (Mike) First, use the Euclidean algorithm to find $\gcd(13, 1000)$:

$$1000 = 13(76) + 12$$
$$13 = 12(1) + 1$$

So $1 = \gcd(13, 1000)$. For the back substitution, let $a = 1000$ and $b = 13$:

$$a = b(76) + 12 \implies 12 = a - 76b$$
$$b = (a - 76b)(1) + 1 \implies 1 = 77b - a$$

Thus, $77(13) + 1000(-1) = 1$ which implies $(77)(13) \equiv 1 \pmod{1000}$. Hence, $13^{-1} \equiv 77 \pmod{1000}$.

Example: Let's use the above inverse to solve the following equation for x:

$$13x + 88 \equiv 762 \pmod{1000}.$$

First, we subtract 762 from both sides to obtain:

$$13x \equiv 238 \pmod{1000}.$$

Now multiply both sides 77, which is the inverse of 13 modulo 1000:

$$\begin{aligned} x &\equiv (77)(13)x \pmod{1000} \\ &\equiv (77)(236) \pmod{1000} \\ &\equiv 18326 \pmod{1000} \\ &\equiv 326 \pmod{1000} \end{aligned}$$

Hence, $x \equiv 326 \pmod{1000}$ is the solution.

No homework for Tuesday except to work on Test # 5.

19. A first look at cryptography

We began class by solving another modular equation:

Example: Solve $47x \equiv 120 \pmod{1000}$

Answer: (Rachel) Note that 47 is prime and does not divide 1000. Therefore, $\gcd(47, 1000) = 1$. Hence, 47 has an inverse modulo 1000. To find the inverse, we need to find a solution to the equation $47x + 1000y = 1$. To do this, we implement the Euclidean algorithm:

$$\begin{aligned} 1000 &= 47(21) + 13 \\ 47 &= 13(3) + 8 \\ 13 &= 8(1) + 5 \\ 8 &= 5(1) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \end{aligned}$$

For the back substitution, let $a = 1000$ and $b = 47$:

$$\begin{aligned} a = b(21) + 13 &\implies 13 = a - 21b \\ b = (a - 21b)(3) + 8 &\implies 8 = 64b - 3a \\ a - 21b = (64b - 3a)(1) + 5 &\implies 5 = 4a - 85b \\ 64b - 3a = (4a - 85b)(1) + 3 &\implies 3 = 67 = 149b - 7a \\ 4a - 85b = (149b - 7a)(1) + 2 &\implies 2 = 11a - 234b \\ 149b - 7a = (11a - 234b)(1) + 1 &\implies 1 = 383b - 18a \end{aligned}$$

Thus, $47(383) + 1000(-18) = 1$ which implies $(383)(47) \equiv 1 \pmod{1000}$. Hence, $47^{-1} \equiv 383 \pmod{1000}$. Now, multiplying both sides of the original equation, we have

$$(383)(47x) \equiv (383)(120) \pmod{1000},$$

which reduces to

$$x \equiv 960 \pmod{1000}.$$

We also made the following remark:

Remark: Suppose $\gcd(a, m) = 1$ and $1 \leq b, c \leq m - 1$. Suppose b and c are both inverses of a modulo m. Then $b = c$. Hence, there is only one inverse of a modulo m (when we reduce to the remainder modulo m).

Proof: Since $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$, we have

$$\begin{aligned} b &\equiv 1 \cdot b \pmod{m} \\ &\equiv (ac)b \pmod{m} \\ &\equiv c(ab) \pmod{m} \\ &\equiv c \cdot 1 \pmod{m} \\ &\equiv c \pmod{m}. \end{aligned}$$

Thus, $b \equiv c \pmod{m}$. Since b and c are between 1 and $m-1$, we must have $b = c$. □

Next, Erica showed that if a has an inverse modulo m, then $\gcd(a, m) = 1$:

Theorem: Let a and m be integers, with $m \geq 2$, and suppose a has an inverse modulo m. Then $\gcd(a, m) = 1$.

Proof: (Erica) Let $d = \gcd(a, m)$. We want to show $d = 1$, or equivalently (since $d > 0$), that $d | 1$. Let b be an inverse of a modulo m. Then $ba \equiv 1 \pmod{m}$. This means that $m | ba - 1$, so $my = ba - 1$ for some integer y. Rewriting this equation, we have $1 = ba - my$. Now, d divides a and m, so d divides ba and my. Thus, d divides $ba - my = 1$. □

Next, we began discussion of our first application of modular arithmetic: cryptography. The science of cryptography deals with sending and receiving coded messages. Not only governments, but also financial institutions and businesses need frequently to transfer sensitive information from one user or from one computer to another in such a way that even if a message is intercepted by the wrong party, it cannot be read. The general public also needs secure methods of transmitting information, so that, for example, a credit card purchase made over the Internet does not allow one's name and credit card number to fall into the hands of an unscrupulous thief.

We use the term *cipher* to mean a system for encoding and decoding messages. We use the term *encryption* to denote the process of transforming ("encoding") a plain text message into a coded message and the term *decryption* to denote the process of transforming ("decoding") the coded message back into the original plain text message. All modern ciphers are based on mathematics and many are based on techniques and results from number theory.

Historically, people have not only used ciphers to keep their messages secret, but they also have devised ways to keep people from knowing that a message was even being sent. An example of a very old and very simple cipher, based on number theory and purportedly used by Julius Caesar, is the so-called *Caesar Cipher*. The idea of the Caesar cipher was to use a simple shift of letters. Replace every letter in the plain text message by the letter three letters to the right to get the coded message. To decode the coded message, one needs only replace each letter in the coded message by the letter three places to the left. The correspondence is shown in the table below.

Cleartext:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ciphertext:	D E F G H I J K L M N O P Q R S T U V W X Y X A B C

For example, the word **CAB** would be encrypted as **FDE**. This is obviously not a very sophisticated system and would be relatively easy to crack if the message was longer than a few letters.

When discussing cryptography, one usually translates letters to numbers via the following scheme:

Letters:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Numbers:	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

Letters:	Q	R	S	T	U	V	W	X	Y	Z
Numbers:	16	17	18	19	20	21	22	23	24	25

Note that if we translate letters to numbers, the Caesar cipher amounts to adding 3 and working modulo 26. For example, to encrypting the letter **U** we add 3 to **20** and get **23**, which corresponds to **X**. To encrypt **Y**, we add 3 to **24** and get **27**, which is **1** modulo 26, corresponding to the letter **B**. To make this precise, the encryption function ϵ for the Caesar cipher is

$$\epsilon(m) = (m+3)\,\%26$$

and the decryption function δ for the Caesar cipher is given by

$$\delta(m) = (m-3)\,\%26.$$

Notice that δ is the *inverse function* for ϵ. In other words, for any message m, we have

$$\delta(\epsilon(m)) = \delta((m+3)\,\%26) = ((m+3)-3)\,\%26 = m.$$

In general, a *shift cipher* is described mathematically by $\epsilon(x) = (x+b)\,\%26$ for some chosen integer b. The decryption function is then given by $\delta(x) = (x-b)\,\%26$. You can check for yourself that $\delta(\epsilon(x)) = x$ for any message x.

To facilitate discussions in cryptography, we usually assume there are two individuals — Alice and Bob — who are wanting to communicate privately, without their opponent — Oscar — knowing what they are saying to each other. We assume that Oscar has full access to the encrypted messages, however. Of course, we also assume that Oscar knows how to translate letters into numbers and conversely. Shift ciphers are far from secure for several reasons. First, there are only 26 possible shift ciphers, so if we assume that Oscar knows that Alice and Bob are using a shift cipher, it is very easy for him to figure out which one it is. Second, Oscar has only to correctly guess one letter correspondence (which would reveal the value of b) to crack the whole code.

We can take a step up in complexity from shift ciphers by considering *affine ciphers*. The idea here is that the encoding function ϵ has two parameters: a and b. We must choose a so that $\gcd(a, 26) = 1$, but b can be any integer. Then $\epsilon(x) = (ax+b)\,\%26$. Let's consider an example:

Example: Consider the affine cipher described by $\epsilon(x) = (5x+11)\,\%26$. We have, for example, $\epsilon(4) = (5(4)+11)\,\%26 = 5$, so the letter **E** is encrypted as **F**.

Question: Suppose you intercept the message **PDQZPSFA** which was encrypted using the affine cipher $\epsilon(x) = (5x+11)\,\%26$. Find the decryption function and use it to decrypt the message.

Let δ be the decryption function. Note that δ is the inverse function of ϵ, i.e., the function δ such that $\delta(\epsilon(x)) = x$ for any input x. How do we find $\delta(x)$? Actually, it's the same method you use to find inverse functions of real numbers.

Start with $y = \epsilon(x) = 5x + 11 \,\%26$. Now interchange the roles of x and y: $x = 5y + 11 \,\%26$. We want to solve for y in terms of x. Subtracting 11 from both sides, we have $5y \equiv x - 11 \pmod{26}$. To get y by itself on the left-hand side, we need to "divide" by 5. In the modular world, we do this by multiplying by the inverse of 5 modulo 26. (This is why we require $\gcd(a, 26) = 1$ in the definition of affine ciphers.) We quickly calculated the inverse of 5 modulo 26 to be 21. That is, $21(5) \equiv 1 \pmod{26}$. Multiplying both sides of our equation by 21, we get $y \equiv 21(x - 11) \equiv 21x + 3 \pmod{26}$. Thus, $\delta(x) = 21x + 3 \,\%26$. Once we have the decryption function, we can quickly decode each letter. E.g., the first letter **P** gets translated as the number 15. Then $\delta(15) = 21(15) + 3 \,\%26 = 6$, which translates to **G**.

Homework:

(1) Decode the message **PDQZPSFA** using the decryption function $\delta(x) = 21x + 3 \,\%26$.

20. Public Key Cryptography and RSA

Erica started out by giving the answer to the homework question from last time:

Example: Decode the message **PDQZPSFA** using the decryption function $\delta(x) = 21x + 3 \,\%26$.

The answer is **GO BIG RED**. For example, the letter **P** corresponds to the number 15, and 15 decodes as $\epsilon(15) = (21)(15) + 3 \,\%26 = 6$, and 6 corresponds to the letter **G**. One treats the rest of the message similarly.

We then returned to our discussion of ciphers. Although there are many more affine ciphers than shift ciphers (how many more?), they are really not that much more secure. Eve has only to make two educated guesses (instead of one) and he can recover the value of a and b in the encryption function $\epsilon(m)$. Once he has the encryption function, he can calculate the decryption function just as we did in the examples above. Both shift ciphers and affine ciphers are examples of *substitution* ciphers, where the ciphertext alphabet is just some (possibly random) permutation of the cleartext alphabet. A serious drawback to substitution ciphers is that one can use common knowledge about the English language (for example, the fact that "e" is by far the most common letter) to make guesses about what the various letters stand for. The "CRYPTOQUOTES" puzzles you find in the newspaper are examples of substitution ciphers.

One might consider encoding more than one letter at a time. For example, suppose we wish to encode 4 letters as one "block". We can still translate each letter into a two-digit number as above, but then we consider the four letters together as an eight-digit number m. Such a number is certainly less than 10^8, so we can use 10^8 as our modulus and proceed as before with our affine cipher. Choose parameters a and b with $\gcd(a, 10^8) = 1$, and set $\epsilon(m) = (am + b) \,\%10^8$. The frequencies for blocks of four letters are not nearly so well known as they are for individual letters, and so this type of affine cipher is much more secure.

There are still problems, however. The main problem is that before Alice and Bob can communicate using this affine cipher, they must decide on the values of a and b. (These values are called the "key" for the cipher.) They can't just send these values to each other unencrypted, because then Eve could read them and he would know the formula for ϵ. So how do Alice and Bob decide on their key?

One solution is to use *public key cryptography*. The basic idea of a public key system is that even if Oscar knows ϵ, he can't figure out δ. In the RSA cyptosystem, which is the public key system we will focus on, the encryption function has the form

$$\epsilon(x) = x^e \,\%N$$

where e and N are carefully chosen positive integers. It turns out that the decrypting function has the same form: $\delta(x) = x^d \,\%N$. In general, given such an ϵ it is very difficult to find δ in any reasonable amount of time, even with the world's fastest computers. However, Alice chooses N in such a way that she (and only she) can quickly compute δ. The secret lies in the prime factorization of N. Here is how it works:

Pick primes:: The first step for Alice is to pick two prime numbers p and q with $p \neq q$. In practice, these primes need to be very large — about 150 digits each– for the cipher to be secure.

- We'll take $p = 7919$ and $q = 7937$.

Calculate n and k:: Next Alice simply sets $N := pq$ and $k = (p-1)(q-1)$. Since Alice knows the factorization of n, she can compute k easily. Notice that in practice, n will have at least 300 digits. This means that computing k would be very difficult without knowing the factorization of N, and factoring N would also be very difficult.

- In our example, we have $N = (7919)(7937) = 62853103$ and $k = (7918)(7936) = 62837248$.

Choose e — the encoding exponent:: The next step is to pick a value of e at random, making sure that $\gcd(e, k) = 1$. Alice does this by first selecting a value for e and then performing the Euclidean Algorithm to calculate $\gcd(e, k)$. If this gcd is 1, great. Otherwise, Alice simply chooses a new value of e.

- For our example, we'll just take $e = q = 7937$. (We wouldn't want to do this in practice, of course, as it may give away the factorization of N!)

Find d — the decoding exponent:: Now, Alice needs to find a value of d so that $de \equiv 1 \pmod{k}$. She can do this through using the Euclidean Algorithm and back substitution. This could be done by hand for small primes such as mine, but in practice we would do this on a computer.

- Using Maple, I found $d \equiv e^{-1} \equiv 49607937 \pmod{k}$.

When all is said and done, Alice's public keys are N and e, and her private key is d. The encoding function, which anyone in the world can use to send a message to Alice, is $\epsilon(x) = x^e \,\%N$. The decoding function, which only Alice knows, is $\delta(x) = x^d \,\%N$. Since in our example N is eight digits long and we want our messages to be less than N (so they will be remainders modulo N), we should break our message into four letter blocks and encode each of these blocks separately. For example, if we wanted to encode the word **MATH**, we plug $m = 12001907$ into our encryption function to get

$$\epsilon(12001907) = 12001907^{7937} \,\%62858103 = 53218748.$$

One can also check (again, using a computer) that

$$\delta(53218748) = (53218748)^{49607937} \,\%62858103 = 12001907.$$

So we see that the decryption function works (for this message, anyway).

Let's try another example:

Example: Suppose $p = 53$ and $q = 71$. Find the encryption and decryption functions, with $e = q$. Encode and decode the two-letter word **BO**.

Here, $N = (53)(71) = 3763$. Since $e = q$, the encryption function is:

$$\epsilon(x) = x^{71} \,\%3763.$$

Now, **BO** corresponds to the four digit number 0114. Gabe did the grunge work and found that $\epsilon(114) = (114)^{71} \,\%3763 = 1463$. To find the decryption function, we need to find the inverse of e modulo k, where $k = (p-1)(q-1) = (52)(70) = 3640$. Mike did the work here (using the Euclidean Algorithm and back substitution) and found

that

$$2871 \equiv 71^{-1} \pmod{3640}.$$

Thus, the decryption function is

$$\delta(x) = x^{2871} \pmod{3763}.$$

To check that $\delta(x)$ does indeed correctly decrypt $\epsilon(114) = 1463$, once again Gabe did the grinding (with checks from Lisa and Huy) to show that

$$\delta(1463) = (1463)^{2871} \,\%3763 = 114.$$

So δ does appear to be the inverse function for $\epsilon(x)$. (The chances that it is not and we just got lucky here are very small indeed!). So why does this work? Next time, we'll prove that that $\delta(\epsilon(x)) = x$ for all x.

Here is your homework for Tuesday:

Homework: Suppose $\epsilon(x) = x^{4007} \,\%6319$ is the encryption function. Find the decryption function $\delta(x)$.

21. More on RSA

We began with the homework problem. Ryan presented the solution.

Problem: Suppose $\epsilon(x) = x^{4007}\,\%6319$ is the encryption function. Find the decryption function $\delta(x)$.

Solution: (Ryan) For starters, Ryan used his calculator program to factor N into primes: $6319 = 71 \cdot 89$. Therefore, $k = (71-1)(89-1) = 6160$. Now, the decryption exponent d is just the inverse of 4007 modulo 6160. One can use the Euclidean Algorithm to find this inverse:

$$\begin{aligned} 6160 &= 1(4007) + 2153 \\ 4007 &= 1(2153) + 1854 \\ 2153 &= 1854(1) + 299 \\ 1854 &= 6(299) + 60 \\ 299 &= 4(60) + 59 \\ 60 &= 1(59) + 1 \end{aligned}$$

Using back substitution, Ryan found that $1 = 103(4007) - 67(6160)$. (We've done this many times before, so I did not write out the work this time.) Hence, $103 \cdot 4007 \equiv 1 \pmod{6160}$, so $103 \equiv 4007^{-1} \pmod{6160}$. Therefore, $d = 103$ is the decryption exponent. So $\delta(x) = x^{103}\,\%6319$.

From the above example we see that one can find the decryption exponent fairly quickly once we've found the prime factorization of N. Even for very large values of N (several hundred digits long), a computer can efficiently implement the Euclidean algorithm to find the inverse of an element once the prime factors of N have been identified. The security of this cryptosystem lies in the fact that there is no known *efficient* method for finding the prime factorization of N if N is a very large integer (at least 300 digits long). Thus, even if Eve knows the value of N and e, he cannot find the decryption exponent (as Ryan did above) until he first finds the prime factorization of N. This could take hundreds or thousands of years using the fastest computers if N is large! On the other hand, it is fairly effortless for a computer to find large primes and multiply them together. So Alice can easily "cook up" a large N to use as her public key so that only she will know the prime factorization. Hence, Alice will be the only one who can decrypt messages using her keys, even though everyone knows how to encrypt using her keys! This is the beauty (and utility) of public key cryptography.

We then gave a proof of why RSA works. Recall that set-up for this cryptosystem: Let p and q be distinct primes, $N = pq$, $k = (p-1)(q-1)$, e any positive integer relatively prime to k, and $d = e^{-1}\,\%k$. Then $\epsilon(x) = x^e\,\%N$ is the encryption function and $\delta(x) = x^d\,\%N$ is the decryption function. We need to prove that for all x, $\delta(\epsilon(x)) = x$; that is, $x^{ed}\,\%N = x$. Thus, we need to prove that $x^{ed} \equiv x \pmod{N}$.

Theorem: Let p, q, N, k, e, d be chosen as above. Then $x^{ed} \equiv x \pmod{N}$ for all integers x.

Proof: (Erica, Megan, Gabe) First, since $N = pq$ and p and q are distinct primes, Megan pointed out that by a previous homework problem it suffices to prove that $x^{ed} \equiv x \pmod{p}$ and $x^{ed} \equiv x \pmod{q}$. We focus on showing $x^{ed} \equiv x \pmod{p}$. The proof for mod q is exactly the same. If $p \mid x$ then certainly (as Gabe mentioned) $p \mid x^{ed}$, and therefore both x and x^{ed} are congruent to zero modulo p. So let's assume for the remainder of this proof that p does not divide x. This is where Erica took over: As $d \equiv e^{-1} \pmod{k}$, we know that $ed \equiv 1 \pmod{k}$. Therefore $ed = k\ell + 1$ for some integer ℓ. Since $k = (p-1)(q-1)$, we have $ed = (p-1)(q-1)\ell + 1$. Now, recall that Fermat's Theorem says that if p does not divide x then $x^{p-1} \equiv 1 \pmod{p}$. Then we get

$$\begin{aligned} x^{ed} &= x^{(p-1)(q-1)\ell+1} \\ &= x \cdot (x^{p-1})^{(q-1)\ell} \\ &\equiv x \cdot (1)^{(q-1)\ell} \\ &\equiv x \end{aligned}$$

Hence, we see that $x^{ed} \equiv x \pmod{p}$. □

We next moved on to a new topic.

Definition: Let $m \geq 2$ be an integer. We define $\phi(m)$ to be the number of integers a in the range $1 \leq a \leq m$ such that $\gcd(a, m) = 1$. The function ϕ is called the *Euler ϕ- function.*

Problem: For $m = 1, 2, \ldots, 16$, find all values of a between 1 and m such that $\gcd(a, m) = 1$. Use this to compute $\phi(m)$. What patterns or conjectures can you make about the ϕ-function?

Everyone helped to fill in the following table:

m	list of all a with $1 \leq a \leq m$ such that $\gcd(a, m) = 1$	$\phi(m)$
1	1	1
2	1	1
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4
11	1,2,3,4,5,6,7,8,9,10	10
12	1,5,7,11	4
13	1,2,3,4,5,6,7,8,9,10,11,12	12
14	1,3,5,9,11,13	6
15	1,2,4,7,8,11,13,14	8
16	1,3,5,7,9,11,13,15	8

Lisa provided us with the first observation:

Theorem: Let p be a prime. Then $\phi(p) = p - 1$.

Proof: (Lisa) All the numbers from 1 to $p - 1$ are relatively prime to p. □

Rachel also noticed a pattern when m is a power of 2:

Theorem: For $\ell \geq 1$ we have $\phi(2^\ell) = \frac{1}{2}(2^\ell) = 2^{\ell-1}$.

Proof: (Rachel) The numbers which are relatively prime to 2^ℓ are precisely all odd numbers. So $\phi(2^\ell)$ is the number of odd integers between 1 and 2^ℓ. Since half of the numbers in this interval are odd and half are even, we get $\phi(2^\ell) = \frac{1}{2}(2^\ell) = 2^{\ell-1}$. □

Next, Megan conjectured the value of $\phi(3^\ell)$ for $\ell \geq 1$.

Theorem: For $\ell \geq 1$, $\phi(3^\ell) = 3^\ell - 3^{\ell-1}$.

Proof: (Megan) Consider the set of integers from 1 up to 3^ℓ. An integer is relatively prime to 3^ℓ if and only if it is not a multiple of 3. But every third integer is a multiple of 3. Thus, one-third of the integers from 1 to 3^ℓ are multiples of 3, leaving two-thirds which are not multiples of 3. Thus,

$$\phi(3^\ell) = \frac{2}{3}(3^\ell) = (2)(3^{\ell-1}) = (3-1)(3^\ell - 1) = 3^\ell - 3^{\ell-1}.$$

Example: $\phi(3^5) = 3^5 - 3^4 = 3^4(3-1) = 81(2) = 162$. Thus, there are 162 integers between 0 and 242 which are relatively prime to 3.

Actually, as both Gabe and Megan pointed out, it's easy to see that this proof generalizes to any prime p:

Theorem: Let p be a positive prime and $\ell \geq 1$. Then

$$\begin{aligned}\phi(p^\ell) &= p^\ell - p^{\ell-1} \\ &= (p-1)p^{\ell-1}.\end{aligned}$$

Proof: (Gabe, Megan) We follow the same logic as with the case $p = 3$. We start with the set of integers from 1 up to p^ℓ. A number in this list is relatively prime to p^ℓ if and only if it is not a multiple of p. Exactly one out of every p of these numbers is a multiple of p, leaving $\frac{(p-1)}{p}(p^\ell) = (p-1)(p^{\ell-1})$ of the numbers relatively prime to p. □

Here is your homework for Thursday:

Homework: Let p and q be distinct primes. Conjecture a formula for $\phi(pq)$. Then prove your formula is correct.

22. The Euler ϕ-function

We began with a discussion of the homework problem. Lisa A. and Gabe came up with the correct formula for $\phi(pq)$, where p and q are distinct primes. The class as a whole provided the proof:

Theorem: Let p and q be distinct primes. Then $\phi(pq) = (p-1)(q-1) = pq-p-q+1$.

Proof: As in the proof of $\phi(p^\ell)$, we start with the set $\{1, 2, \ldots, pq\}$ and take out all those numbers which are **not** relatively prime to pq. An integer is not relatively prime to pq if and only if it is a multiple of p or q (or both). Since every pth integer is a multiple of p and the list ends with a multiple of p, we conclude that there are $\frac{1}{p}(pq) = q$ integers in the list which are multiples of p. By the same reasoning, there are $\frac{1}{q}(pq) = p$ multiples of q in the list. However, we've counted pq twice as it is a multiple of both p and q. Since p and q are primes, pq is the *only* number in our range which is a multiple of both p and q. Thus,

$$\begin{aligned}\phi(pq) &= pq - (\#\text{ of multiples of } p) - (\#\text{ of multiples of } q) + (\#\text{ of multiples of } pq)\\ &= pq - q - p + 1\\ &= (p-1)(q-1).\end{aligned}$$

□

Next, we applied the same reasoning to get a formula for $\phi(pqr)$, where p, q and r are distinct primes?

Theorem: Let p, q and r be distinct primes. Then

$$\phi(pqr) = pqr - pr - pr - qr + p + q + r - 1 = (p-1)(q-1)(r-1).$$

Proof: Reasoning as before, we start with the list $\{1, 2, \ldots, pqr\}$. We want to subtract out all integers in this list which are not relatively prime to pqr, i.e., integers which are multiples of p or q or r. As before, we get $\frac{1}{p}(pqr) = qr$ multiples of p, $\frac{1}{q}(pqr) = pr$ multiples of q, and $\frac{1}{r}(pqr) = pq$ multiples of r. We subtract them out to get $pqr - qr - pr - pr$. But, we've counted multiples of pq twice (since they are multiples of both p and q) and there are $\frac{1}{pq}(pqr) = r$ of those. So we add r back to the total. Similarly, we counted the multiples of pr (q of them) and qr (p of them) back in, to get $pqr - pq - qr - pr + p + q + r$. Finally, in our 'adding back in stage', we added the multiples of pqr (of which there is only one) back in 3 times (being a multiple of pq, pr and qr) after it was subtracted out 3 times (being a multiple of p, q, and r). So we still need to subtract it out, since it is not relatively prime to pqr. Thus, our final number for the number of integers between 1 and pqr which are relatively prime to pqr is

$$pqr - pq - pr - qr + p + q + r - 1.$$

□

We can also use this reasoning to do more cases, such as $\phi(pqrs)$ where p,q, r, and s are distinct primes. However, the arguments become increasingly more complicated. Instead, we will get a general formula by a different route. For now, we will just state the formula and prove it later:

Theorem: Let $m = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ be the prime factorization of m, where $p_1, \ldots, p_t$ are distinct primes. Then

$$\begin{aligned}\phi(m) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_t^{k_t}) \\ &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_t^{k_t} - p_t^{k_t-1}).\end{aligned}$$

Example: Assuming the above formula is true, then $\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 4 \cdot 120 = 480$. Thus, there are 480 integers between 1 and 1000 which are relatively prime to 1000.

Next, we did another numerical experiment: We calculated the value of $a^{\phi(m)} \pmod m$ for various values of m and a with $\gcd(a, m) = 1$. For example, we found:

$$\begin{aligned} 4^{\phi(9)} &\equiv 1 \pmod 9 \\ 9^{\phi(14)} &\equiv 1 \pmod{14} \\ 2^{\phi(15)} &\equiv 1 \pmod{15} \\ 11^{\phi(16)} &\equiv 1 \pmod{16} \end{aligned}$$

If we tried values of a which were not relatively prime to m, we got entirely different results:

$$\begin{aligned} 3^{\phi(9)} &\equiv 0 \pmod 9 \\ 7^{\phi(14)} &\equiv 7 \pmod{14} \\ 3^{\phi(15)} &\equiv 12 \pmod{15} \end{aligned}$$

Ryan made the following conjecture:

Conjecture: (Ryan) Let $m \geq 2$ be an integer and $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod m$.

Huy noticed that this conjecture looks similar to Fermat's (Little) Theorem: If p is prime and $a \not\equiv 0 \pmod p$ then $a^{p-1} \equiv 1 \pmod p$. In fact, if $m = p$ in the above conjecture, we get exactly Fermat's Theorem, since $\phi(p) = p - 1$ and $\gcd(a, p) = 1$ if and only if $a \not\equiv 0 \pmod p$.

Next,we set out to prove Ryan's conjecture. To do so, we attempted to mimic the (second) proof we gave for Fermat's Theorem. We reintroduced some notation:

For an integer $m \geq 2$, we let S_m be the set of integers between 1 and $m - 1$ which are relatively prime to m. For example, we have:

$$S_4 = \{1, 3\}$$
$$S_8 = \{1, 3, 5, 7\}$$
$$S_9 = \{1, 2, 4, 5, 7, 8\}$$
$$S_{10} = \{1, 3, 7, 9\}$$

In general, we know there are $\phi(m)$ elements in S_m, so we can write the set S_m as $\{x_1, x_2, \ldots, x_{\phi(m)}\}$. If we wrote these elements in ascending order (there is no real reason to, however), we would have $x_1 = 1$ and $x_{\phi(m)} = m - 1$.

Now let $a \in S_m$; i.e., $\gcd(a, m) = 1$. We claim that for all $x \in S_m$, $ax \,\%m \in S_m$. To see this, suppose not. Let $r = ax \,\%m$. Certainly r is between 0 and $m - 1$. So if $r \notin S_m$, we must have $\gcd(r, m) > 1$. This means there is a prime p such that p divides both r and m. Now, since $r = ax \,\%m$, we have $ax = mq + r$ for some $q \in \mathbb{Z}$. Since p divides both m and r, p divides $mq + r$ and hence ax. But since p is prime, this means that p divides a or p divides x. But this can't happen, since $\gcd(a, m) = 1$ and $\gcd(x, m) = 1$. Thus, we must have $\gcd(r, m) = 1$.

As with the proof of Fermat's Theorem, for $a \in S_m$ define a function $f_m^a : S_m \to S_m$ by $f_m^a(x) = ax \,\%m$ for each $m \in S_m$. By the preceeding paragraph, since $\gcd(ax \,\%m, m) = 1$, we have $f_m^a(x) \in S_m$.

Let's do an example with $m = 9$. We have $S_9 = \{1, 2, 4, 5, 7, 8\}$. Choose a random element in S_9, say 4. Then

$$f_9^4(1) = 4 \cdot 1 \,\%9 = 4$$
$$f_9^4(2) = 4 \cdot 2 \,\%9 = 8$$
$$f_9^4(4) = 4 \cdot 4 \,\%9 = 7$$
$$f_9^4(5) = 4 \cdot 5 \,\%9 = 2$$
$$f_9^4(7) = 4 \cdot 7 \,\%9 = 1$$
$$f_9^4(8) = 4 \cdot 8 \,\%9 = 5$$

Notice that, just as with the case $m = p$ is prime (which we did before) every element in S_9 was 'hit'; that is, the map is one-to-one and onto.

We made the following conjecture

Conjecture: Suppose m is prime and $a \in S_m$. Then the map $f_m^a : S_m \to S_m$ is one-to-one and onto.

Mimicking the proof from the case $m = p$ is prime, we were able to prove this conjecture.

Proof: By the Pigeonhole Principle, it suffices to prove that f_m^a is one-to-one. Suppose $f_m^a i) = f_m^a(j)$ for some elements $i \neq j$ in S_m. Then $ai \,\%m = aj \,\%m$, which means $ai \equiv aj \pmod{m}$. Since $\gcd(a, m) = 1$, by cancellation we have that $i \equiv j \pmod{p}$. But, since i and j are between 1 and $m - 1$, this means that $i = j$, a contradiction. Hence, f_m^a must be one-to-one (and thus onto). □

We now are in a position to prove Ryan's conjecture (again, mimicking the proof from Fermat's Theorem). The result is known as *Euler's Theorem*:

Theorem: (Euler's Theorem) Let $m \geq 2$ be an integer and a an integer such that $\gcd(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof: It is enough to prove this in the case $a \in S_m$, since by the reasoning above (three paragraphs ago) a is relatively prime to m if and only if its remainder upon dividing a by m is relatively prime to m. By the conjecture above, $f_m^a : S_m \to S_m$ is one-to-one and onto, we have

$$\begin{aligned} S_p &= \{x_1, x_2, \ldots, x_{\phi(m)}\} \\ &= \{f_m^a(x_1), f_m^a(x_2), \ldots, f_m^a(x_{\phi(m)})\} \\ &= \{ax_1 \,\%m, ax_2 \,\%m, \ldots, ax_{\phi(m)} \,\%m\} \end{aligned}$$

Since the elements in these sets are the same (with just the order scrambled), the products of their elements are the same:

$$x_1 x_2 \cdots x_{\phi(m)} = (ax_1 \,\%m)(ax_2 \,\%m) \cdots (ax_{\phi(m)} \,\%m).$$

Instead of using the '% m' notation, we can instead write this as a modular equation:

$$\begin{aligned} x_1 x_2 \cdots x_{\phi(m)} &\equiv (ax_1)(ax_2) \cdots (ax_{\phi(m)}) \pmod{m} \\ &\equiv x_1 x_2 \cdots x_{\phi(m)} a^{\phi(m)} \pmod{m} \end{aligned}$$

Since each x_i is relatively prime to m, we can cancel it from both sides of the modular equation. (Equivalently, we could multiply both sides of the equation by the inverse of x_i.) Doing this for all x_i, we obtain:

$$1 \equiv a^{\phi(m)} \pmod{m}.$$

□

There was no homework assigned for Tuesday.

23. The Chinese Remainder Theorem

Our goal for the next two class periods (Today and next Tuesday) is to prove the following theorem:

Theorem: Let $m = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ be the prime factorization of m, where $p_1, \ldots, p_t$ are distinct primes. Then

$$\begin{aligned}\phi(m) &= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_t^{k_t}) \\ &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_t^{k_t} - p_t^{k_t-1}).\end{aligned}$$

The key to proving this theorem lies in the Chinese Remainder Theorem, which says the following:

Theorem: (The Chinese Remainder Theorem) Let m and n be relatively prime positive integers and u and v any integers. Then there exists a unique integer x with $1 \leq x \leq mn$ such that

$$\begin{aligned} x &\equiv u \pmod{m}, \text{ and} \\ x &\equiv v \pmod{n}. \end{aligned}$$

Here is an example of the Chinese Remainder Theorem in use:

Example: Let $m = 10$, $n = 11$, $u = 72$ and $v = 5943$. The Chinese Remainder Theorem says that there exists a unique integer x between 1 and 110 such that $x \equiv 72 \pmod{10}$ and $x \equiv 6543 \pmod{11}$. Reducing u and v, we want $x \equiv 2 \pmod{10}$ and $x \equiv 3 \pmod{11}$. By trial and error we can see that $x = 102$ works.

To prove the Chinese Remainder Theorem, we first introduce some new notation. Let m and n be positive integers. We'll define two sets:

$$S_{mn} := \{1, 2, 3, \ldots, mn\}$$

and

$$T_{m,n} := \{(a, b) \mid 0 \leq a \leq m-1,\ 0 \leq b \leq n-1\}.$$

Example: Suppose $m = 2$ and $n = 3$. Then

$$S_6 = \{1, 2, 3, 4, 5, 6\}$$

and

$$T_{2,3} = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Notice that S and T both have exactly mn elements. This is easy to see for S. For T, think of the ordered pairs as lattice points in the plane $\mathbb{R}^2$. (A lattice point is just a point in $\mathbb{R}^2$ whose x- and y-coordinates are integers.) The points of T form a grid or matrix having m columns and n rows. Thus, there are mn lattice points in this grid.

We now define a function $f_{m,n}$ from S_{mn} to $T_{m,n}$ as follows:

$$f_{m,n} : S \to T \qquad \text{is defined by} \qquad f_{m,n}(x) = (x\,\%m, x\,\%n).$$

That is, the first coordinate of $f_{m,n}(x)$ is the remainder upon dividing x by m; the second coordinate is the remainder upon dividing x by n. Since the remainders when you divide by m and n are between, respectively, 0 and $m-1$, and 0 and $n-1$, the ordered pair we get is indeed a member of the set T.

Let's look at an example:

Example: Suppose $m = 2$ and $n = 3$. Let's compute the function $f_{2,3}$ for every element of S_6:

$$\begin{aligned}
f_{2,3}(1) &= (1\,\%2, 1\,\%3) = (1,1)\\
f_{2,3}(2) &= (2\,\%2, 2\,\%3) = (0,2)\\
f_{2,3}(3) &= (3\,\%2, 3\,\%3) = (1,0)\\
f_{2,3}(4) &= (4\,\%2, 4\,\%3) = (0,1)\\
f_{2,3}(5) &= (5\,\%2, 5\,\%3) = (1,2)\\
f_{2,3}(6) &= (6\,\%2, 6\,\%3) = (0,0)
\end{aligned}$$

Example: Suppose $m = 2$ and $n = 4$. We compute $f_{2,4}$ for every element of S_8:

$$\begin{aligned}
f_{2,4}(1) &= (1\,\%2, 1\,\%4) = (1,1)\\
f_{2,4}(2) &= (2\,\%2, 2\,\%4) = (0,2)\\
f_{2,4}(3) &= (3\,\%2, 3\,\%4) = (1,3)\\
f_{2,4}(4) &= (4\,\%2, 4\,\%4) = (0,0)\\
f_{2,4}(5) &= (5\,\%2, 5\,\%4) = (1,1)\\
f_{2,4}(6) &= (6\,\%2, 6\,\%4) = (0,2)\\
f_{2,4}(7) &= (7\,\%2, 7\,\%4) = (1,3)\\
f_{2,4}(8) &= (8\,\%2, 8\,\%4) = (0,0).
\end{aligned}$$

We proved the following theorem:

Theorem: Let m and n be positive integers. If $\gcd(m,n) = 1$ then $f_{m,n} : S_{mn} \to T_{m,n}$ is both one-to-one and onto. Conversely, if $f_{m,n}$ is one-to-one (and/or onto) then $\gcd(m,n) = 1$.

Proof: We first show that $f_{m,n}$ is one-to-one. Let x, y be integers in the set S_{mn}. We need to show that if $x \neq y$ then $f_{m,n}(x) \neq f_{m,n}(y)$. Equivalently, it is enough to prove the contrapositive: If $f_{m,n}(x) = f_{m,n}(y)$ then $x = y$. So suppose $f_{m,n}(x) = f_{m,n}(y)$. Without loss of generality we can assume $x \geq y$. (One of the numbers must be bigger than or equal to the other.) We are given that $f_{m,n}(x) = f_{m,n}(y)$; i.e., $(x\,\%m, x\,\%n) = (y\,\%m, y\,\%n)$. Since these are ordered pairs, this must mean $x\,\%m = y\,\%m$ and $x\,\%n = y\,\%n$. That is, x and y have the same remainders when divided by m and n. This means $x \equiv y \pmod m$ and $x \equiv y \pmod n$. Therefore, m divides $x - y$ and n divides $x - y$. Since m and n are relatively prime, we must have

mn divides $x - y$. But $1 \leq y \leq x \leq mn$, so $0 \leq x - y < mn$. The only multiple of mn in this range is zero! Hence, $x - y = 0$, or $x = y$. Thus, $f_{m,n}$ is one-to-one.

Since S_{mn} and $T_{m,n}$ have the same number of elements (mn), we now that $f_{m,n}$ by the Pigeonhole Principle.

Now suppose $f_{m,n}$ is one-to-one and onto. We need to show $\gcd(m, n) = 1$. Let $d = \gcd(m, n)$. Then $\frac{mn}{d} \in S_{mn}$ and $\frac{mn}{d} \equiv 0 \pmod{m}$ and $\frac{mn}{d} \equiv 0 \pmod{n}$ (since d divides both m and n). Hence, $f_{m,n}(\frac{mn}{d}) = (0, 0)$. But $f_{m,n}(mn) = (0, 0)$. Since $f_{m,n}$ is one-to-one, we must have $\frac{mn}{d} = mn$. Hence, $d = 1$. □

We can now give a proof of the Chinese Remainder Theorem:

Corollary: (The Chinese Remainder Theorem) Let m and n be relatively prime positive integers and u and v any integers. Then there exists a unique integer x with $1 \leq x \leq mn$ such that

$$x \equiv u \pmod{m}, \text{ and}$$
$$x \equiv v \pmod{n}.$$

Proof: Let $S = \{1, 2, 3, \ldots, mn\}$ and $T = \{(r, s) \mid 0 \leq r \leq m - 1, 0 \leq s \leq n - 1\}$. Let $r = u \,\%m$ and $s = v \,\%n$. Then (r, s) is in the set T and $u \equiv r \pmod{m}$ and $v \equiv s \pmod{n}$. Since the map f is onto, we know that there exists an integer x in the set S such that $f_{m,n}(x) = (x \,\%m, x \,\%n) = (r, s)$. Thus, $x \equiv r \pmod{m}$ and $x \equiv s \pmod{n}$. Thus, $x \equiv u \pmod{m}$ and $x \equiv v \pmod{n}$. Furthermore, there is only one x in the set S which works since $f_{m,n}$ is one-to-one. □

There is no homework for next week except to continue working on the last exam.

24. More on the Chinese Remainder Theorem

Let m and n be positive integers. Last class we defined the sets S_{mn} and $T_{m,n}$ as follows:

$$S_{mn} := \{1, 2, 3, \ldots, mn\}$$

and

$$T_{m,n} := \{(a, b) \mid 0 \leq a \leq m-1,\ 0 \leq b \leq n-1\}.$$

We also defined a function $f_{m,n} : S_{mn} \to T_{m,n}$ by $f(x) = (x\%m, x\%n)$. We then proved that $f_{m,n}$ is one-to-one and onto if and only if $\gcd(m, n) = 1$. This result is a form of the Chinese Remainder Theorem.

Now we are going to restrict the function $f_{m,n}$ to a smaller domain. Let

$$S^*_{mn} := \{x \in S_{mn} \mid \gcd(x, m) = 1\}$$
$$T^*_{m,n} := \{(a, b) \in T_{m,n} \mid \gcd(a, m) = 1, \gcd(b, n) = 1\}.$$

So $S^*_{mn} \subset S_{mn}$ and $T^*_{m,n} \subset T_{m,n}$. Notice by definition of the ϕ that S^*_{mn} has $\phi(mn)$ elements For $T^*_{m,n}$, notice that there are $\phi(m)$ choices for the first coordinate and $\phi(n)$ choices for the second coordinate. This means that $T^*_{m,n}$ has $\phi(m)\phi(n)$ elements.

Example: Let $m = 3$ and $n = 4$. Then

$$S^*_{12} = \{1, 5, 7, 11\}$$
$$T^*_{3,4} = \{(1, 1), (1, 3), (2, 1), (2, 3)\}$$

Now define $f^*_{m,n} : S^*_{mn} \to T_{m,n}$ the same way we did before: for $x \in S^*_{mn}$ define

$$f^*_{m,n}(x) := (x \,\%\, m, x \,\%\, n).$$

Here is a quick example when $m = 3$ and $n = 4$:

$$f^*_{3,4}(1) = (1, 1)$$
$$f^*_{3,4}(5) = (2, 1)$$
$$f^*_{3,4}(7) = (1, 3)$$
$$f^*_{3,4}(11) = (2, 3)$$

Notice that in this example that for all $x \in S^*_{12}$, $f^*_{3,4}(x) \in T^*_{3,4}$, not just in $T_{3,4}$. We would like to prove this in general. To show this, we need to prove that if $\gcd(x, m) = 1$ then $\gcd(x\,\%m, m) = 1$ and $\gcd(x\,\%n, n) = 1$. Let $r = x\,\%m$ and $s = x\,\%n$. Note that $x \equiv r \pmod{m}$ and $x \equiv s \pmod{n}$. What we want now follows from the following lemma, which was proved by Lisa:

Lemma: Let a, b, m be integers with $m > 0$. Suppose $a \equiv b \pmod{m}$. Prove that $\gcd(a, m) = \gcd(b, m)$.

Proof: (Lisa A.) Let $d = \gcd(a, m)$ and $e = \gcd(b, m)$. We need to show $d = e$. By our hypothesis, we have $a - b = mq$ for some integer q. As d divides both a and m, it also divides $b = a - mq$. Thus, d is a common divisor of both b and m and

hence is less than the greatest common divisor of b and m, namely e. So we've proved $d \leq e$. A similar argument shows that $e \leq d$. □

As a consequence of this lemma, we get the following:

Corollary: Let m and n be positive integers and $x \in S^*_{mn}$. Then $f_{m,n}(x) \in T^*_{mn,}$ if and only if $x \in S^*_{mn}$.

Proof: Let $f_{m,n}(x) = (a, b)$, where $a = x\%\, m$ and $b = x\%\, n$. Then $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. Suppose first that $x \in S^*_{mn}$. Then $\gcd(x, mn) = 1$, which implies $\gcd(x, m) = 1$ and $\gcd(x, n) = 1$. By the lemma above, this means $\gcd(a, m) = \gcd(x, m) = 1$ and $\gcd(b, n) = \gcd(x, n) = 1$. Thus, $(a, b) \in T^*_{m,n}$. Conversely, suppose $(a, b) \in T^*_{m,n}$. This means that $\gcd(a, m) = 1$ and $\gcd(b, n) = 1$. Again by the lemma above, we have that $\gcd(x, m) = 1$ and $\gcd(x, n) = 1$. Clearly, this implies $\gcd(x, mn) = 1$ and so $x \in S^*mn$. □

Thus, $f^*_{m,n}$ is a function from S^*_{mn} to $T^*_{m,n}$ (not just $T_{m,n}$). Notice in our example above that $f^*_{3,4}$ is one-to-one and maps onto the set $T^*_{3,4}$. We will show next time that this is always true when $\gcd(m, n) = 1$.

There is no homework for Thursday other than to finish the last exam.

25. The Euler ϕ-function, revisited

Last time, we showed that given two integers m and n there is a function $f^*_{m,n} : S^*_{mn} \to T^*_{m,n}$ given by $f^*_{m,n}(x) = (x\%m, x\%n)$. We now prove that this function if one-to-one and onto whenever $\gcd(m,n) = 1$.

Theorem: Let m and n be relatively prime positive integers. Then $f^*_{m,n} : S^*_{mn} \to T^*_{m,n}$ is one-to-one and onto.

Proof: We will use the fact that the function $f_{m,n} : S_{mn} \to T_{m,n}$ is one-to-one and onto. Suppose $f^*_{m,n}(x) = f^*_{m,n}(y)$ for some $x, y \in S^*_{mn}$. Then certainly $f_{m,n}(x) = f_{mn,}(y)$. Since $f_{m,n}$ is one-to-one, we must have $x = y$. Thus, $f^*_{m,n}$ is also one-to-one.

Now let $(a,b) \in T^*_{m,n}$. As $(a,b) \in T_{m,n}$ and $f_{m,n}$ is onto, there exists an $x \in S_{mn}$ such that $f_{m,n}(x) = (a,b)$. We want to show that $x \in S^*_{mn}$. Since $(a,b) \in T^*_{m,n}$, $\gcd(a,m) = 1$ and $\gcd(b,n) = 1$. Also, $x \equiv a \pmod m$ and $x \equiv b \pmod n$. By the lemma from last class, we get that $\gcd(x,m) = 1$ and $\gcd(x,n) = 1$. Hence, $\gcd(x,mn) = 1$ and so $x \in S^*_{mn}$. Thus, $f^*_{m,n}(x) = f_{m,n}(x) = (a,b)$, which shows that $f^*_{m,n}$ is onto. □

As an immediate corollary, we get the following:

Corollary: Let m and n be relatively prime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.

Proof: By the theorem above, since $f^* : S^*_{mn} \to T^*_{m,n}$ is one-to-one and onto, we have that S^*_{mn} and $T^*_{m,n}$ have the same number of elements. But, by definition of the Euler ϕ-function, the number of elements in S^*_{mn} is $\phi(mn)$ and the number of elements in $T^*_{m,n}$ is $\phi(m)\phi(n)$. Therefore, $\phi(mn) = \phi(m)\phi(n)$. □

Finally, as our last theorem of the course, we get the following result which was proved by Jane:

Theorem: Let $a = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ be the prime factorization of a, where $p_1, \ldots, p_k$ are distinct primes. Then

$$\begin{aligned}\phi(a) &= \phi(p_1^{m_1})\phi(p_2^{m_2}) \cdots \phi(p_k^{m_k}) \\ &= (p_1^{m_1} - p_1^{m_1-1})(p_2^{m_2} - p_2^{m_2-1}) \cdots (p_k^{m_k} - p_k^{m_k-1}).\end{aligned}$$

Proof: (Jane) We use induction on the number k of primes in the prime factorization of a. If $k = 1$ this is just the formula $\phi(p^k) = p^k - p^{k-1}$ proved on November 18th. Now let's assume $k > 1$ and we know theorem is true for $k-1$ prime factors. Let $c = p_k^{m_k}$ and $b = \frac{a}{c} = p_1^{m_1} \cdots p_{k-1}^{m_{k-1}}$. Since $\gcd(b,c) = 1$, we know that $\phi(a) = \phi(bc) = \phi(b)\phi(c) = \phi(b)\phi(p_k^{m_k})$. By our inductive hypothesis, we know $\phi(b) = \phi(p_1^{m_1}) \cdots \phi(p_{k-1}^{m_{k-1}})$. Thus,

$$\phi(a) = \phi(p_1^{m_1}) \cdots \phi(p_k^{m_k}).$$

□

Appendix A. Using Maple

The computer algebra package Maple is very helpful for doing some of the computations we've been doing lately. Here is some of the information we need on using Maple:

Starting Maple and General Rules. All the computers in the math department (so in particular the ones in our classroom) have Maple. From the Start menu, pick Programs, and then find Maple in that list. Just double-click on the right thing and you're ready to go.

Every command must end with a semicolon, and spaces must be used "appropriately". When you want to assign a value to a variable, always use ":=" instead of just "=".

The Extended Euclidean Algorithm. The Extended Euclidean Algorithm is built-in to Maple as `igcdex`. Say you want to find integers u and v such that $5u + 27v = 1$. First, do the following command:

```
igcdex(5,27,'u','v');
```

The output of this command will just be 1, but if you type

```
u;
```

the output will be 11, and if you type

```
v;
```

the output will be -2. (You can check that $(5 \times 11) + (27 \times (-2)) = 1$.) Note that if you want a positive value of x so that $27x \equiv 1 \pmod 5$, you can simply add $5 + (-2)$ to get 3.

Primes. Maple has a very neat function called `nextprime`. When you input

```
nextprime(5342);
```

the output will be 5347. This means that 5347 is the smallest prime which is bigger than 5342. Warning: In general, Maple doesn't know for sure that the number it outputs is prime. However, this number has passed many primality tests, so it's "probably prime". Further, it's likely that enough tests have been done so that the probability that the number is not prime is smaller than the probability your computer has made a mistake!

Modular Arithmetic and Fast Exponentiation. Modular arithmetic and fast exponentiation are also built-in to Maple. For example, the command

```
-57 mod 32;
```

will output 7, since 7 is the unique integer between 0 and 31 which is congruent to -57 modulo 32.

To compute $5983^{84736} \pmod{83726}$, use the command

```
5983 &^ 84736 mod 83726;
```

The "&^" tells Maple to use fast exponentiation, reducing modulo 83726 at each step.

Appendix B. Projects

Each student is required to participate in a joint project with another student. The project will have both a written and an oral component. These projects can be based on interesting problems or applications that were considered in class, but which were not fully explored, or they can be chosen from the list of suggested topics below. Each pair of students will be assigned a presentation date on which they must present the oral component of their project. Additionally, the written component of the project is due on that date. There will be no extensions. Your project will count 20% of your final grade.

Written Component. Your paper should be about 5 to 10 pages long. Quality is more important than quantity. Have something to say and say it clearly and concisely. If you are presenting the results of your investigation of some journal article or textbook chapter, you should fill in the missing parts of each argument or proof and do any problems left to the reader. It would be better to go into a small part of some topic in depth and detail, rather than try to cover a large area superficially. This is your opportunity to show that you can read some mathematics on your own and then explain it in writing to your reader.

On Thursday, October 30th, you will need to tell me who your partner is and which topic you're going to work on. I will announce which group presents on which date the following class period. (All presentations will be during the last week of classes.) The written component is due the day you do your oral presentation.

Oral Presentations. You will have 20 minutes to enlighten your colleagues about the topic you have researched. Your presentation should be clear and to the point. Choose your examples carefully to illustrate the points you want to make. In a group presentation, all in the group should have a role and all should be able to answer any questions which arise. You should rehearse your presentation in advance on some fellow students and leave some time for questions and interruptions. Class presentations always take more time than you think they will. Rehearsal will help you to better gauge how much you can accomplish. Attendance is mandatory for everyone for all oral presentations.

Some Possible Topics.

Check Digit Schemes.: What schemes are used for some specific types of numbers (credit cards, drivers' licenses, passport numbers, shipping labels)? What are the advantages and disadvantages of certain schemes? Why do you think each of these particular schemes was chosen?

Mathematics and Magic.: What are some of the many magicians' tricks, especially with cards, that are built upon number theoretic facts?

The Gregorian Calendar.: How does it work? How long is a complete period before the sequence of days and dates repeats? How can you find the day of the week for any date?

Mathematics and Music.: What does number theory have to do with piano tuning and the "Well-tempered Klavier"? What was Bach's contribution? What number theoretic problems arise in tuning a piano so that it can be played in any key?

Random Number Generation.: How does the built-in the random number generator in your calculator or your favorite computer language or spreadsheet actually work? What are its strengths and shortcomings? How could it be improved?

Perfect Numbers and Mersenne Primes.: What is the history of perfect numbers? What are some of their properties? What precisely is the connection between perfect numbers and Mersenne primes? Do odd perfect numbers exist?

Factoring Methods.: We have used only trial division to factor numbers. What are some of the other techniques available? The Fermat method and the Monte-Carlo (or Pollard rho method) are both accessible to someone with the background of this course.

Primality Tests.: What are some of the tests that are used to determine whether a given number is prime or composite?

Chinese Remainder Theorem.: What does this say, why is it true, and how is it used? How can it be used to perform arithmetic with large numbers?

Continued Fractions.: Consider these strange representations of fractions:

$$\frac{3}{17} = \frac{1}{5 + \frac{1}{1+\frac{1}{2}}} \qquad \text{and} \qquad \frac{24}{31} = \frac{1}{1 + \frac{1}{3+\frac{1}{2+\frac{1}{3}}}}$$

In fact every rational number can be written in this form. What about irrational numbers? Why is expressing things in this way useful?

Geometric Numbers.: We all know the square numbers. What are triangular numbers and pentagonal numbers? What are some of their interesting properties?

Fibonacci Numbers.: These are a source of many interesting patterns and even have a journal devoted to them. What are they and why are they important? The first few are 1, 1, 2, 3, 5, 8, 13, etc.

***p*-adic integers.:** What are p-adic integers? What are some of their properties? What can they be used for?

Resources. You may want to browse through some of the books on Number Theory in the math library. The internet also has many good sites dealing with Number Theoretic topics. Using any of the standard search engines should produce many good references. (Be careful about using websites as references — some are more reliable than others! If you want to use a website as one of your references, you should clear it with me first.) I'm happy to help you find some references if you like.

Appendix C. Take-Home Test 1

Due: Thursday, September 11

Collaboration Allowed

Collaboration on this test is both allowed and encouraged. By collaboration, I mean that you are encouraged to discuss the problems, test out your ideas, check your reasoning and arguments, etc., with other people. *However, there is a big difference between collaborating and copying. Each student must write up his or her own solutions to the problems in his or her own words.*

You will be graded both on mathematical content and on clarity of expression. Each problem is worth a maximum of 12 points. Some of the questions are a bit open-ended, so be creative, make educated guesses if you have to, but back up your assertions by providing proofs, counterexamples, or (in the case of guesses) numerical evidence. In writing your answers, use complete sentences (with punctuation!) and be sure to say exactly what you mean. Papers will be graded on the basis of what you have written, so be sure to take the time to express yourself clearly. If you are stuck on a problem and have no idea where to begin, a good way to get started is to look at lots of specific examples and try to find a pattern.

On this test you have a choice. Do any **five** of the following six problems. You must decide which ones you think you can do best. If you do all six, I will count only the first five—not the best five.

(1) Prove that the set of all odd positive integers can be divided into three classes, depending upon their remainders when divided by 6:
   - All those which are of the form $6n+1$, namely 1, 7, 13, 19, etc. Let's call these the **six-one** integers.
   - All those which are of the form $6n+3$, namely 3, 9, 15, 21, etc. Let's call these the **six-three** integers.
   - All those which are of the form $6n+5$, namely 5, 11, 17, 23, etc. Let's call these the **six-five** integers.

   What kinds of statements can one make about the product of two six-one numbers, two six-three numbers, two six-five numbers, a six-one number and a six-three number, a six-one number and a six-five number, and a six-three number and a six-five number? (We know all these products will be odd, but will they be six-one numbers, six-three numbers, or six-five numbers?) Don't forget proofs!

(2) We say that an ordered triple (a, b, c) of positive integers (written in ascending order) is a *Pythagorean triple* if $a^2 + b^2 = c^2$. There are many examples of Pythagorean triples. For example, $(3, 4, 5)$, $(5, 12, 13)$, and $(6, 8, 10)$ are all Pythagorean triples.
   (a) Show that if (a, b, c) is a Pythagorean triple and d is any positive integer, then (da, db, dc) is a Pythagorean triple.
   (b) Let $a > 1$ be an odd integer. Show that a begins a Pythagorean triple; i.e., there exist positive integers b, c such that (a, b, c) is a Pythagorean triple. (Hint: Let $b = \frac{a^2-1}{2}$.)
   (c) Let a be any positive integer which is not a power of 2. Show that a begins a Pythagorean triple.

(3) Let (a, b, c) be any Pythagorean triple. Prove that a and b cannot both be odd. (Hint: Look at the remainders of a, b, and c when you divide by 4.)

(4) Observe that for the first few positive integers n, the number $n^2 - n$ is a multiple of 2. For example, $1^2 - 1 = 0$, $2^2 - 2 = 2$, $3^2 - 3 = 6$, $4^2 - 4 = 12$, etc. Is this always true? In other words, is $n^2 - n$ always a multiple of 2?

Similarly, the numbers $1^3 - 1 = 0$, $2^3 - 2 = 6$, $3^3 - 3 = 24$, $4^3 - 4 = 60$, etc., all seem to be multiples of 3. Is this always true? In other words, is $n^3 - n$ always a multiple of 3?

Does this hold more generally? In other words, if n and k are positive integers, will $n^k - n$ always be a multiple of k?

(5) List all the possible (positive) divisors of the integers from 1 to 30. For example, 12 has the six divisors 1, 2, 3, 4, 6, and 12. You will notice that "most" positive integers have an even number of divisors, but a few have an odd number of divisors. Classify those positive integers which have an even number of divisors and those which have an odd number of divisors. Try to explain why your classification works in general.

(6) Fun with gcd's. Let a and b be positive integers.
   (a) Prove or disprove: If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.
   (b) Prove: $\gcd(a, a + 2) = 1$ or 2. For which values of a is $\gcd(a, a + 2) = 2$?
   (c) Suppose $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Must $\gcd(a, b) = 1$? Similarly, if $ax + by = 2$ must $\gcd(a, b) = 2$?

Statement of Sources: : Give a list of all people with whom you discussed the problems on this test. Also, if you used any references besides the class notes, list them as well.

Appendix D. Take-Home Test 2

Due: Thursday, September 25

Solo – No Collaboration Allowed

On this test, your work is to be your own with no consultation with any other person (in this class or not) except for the instructor. Feel free to ask me any questions. I won't give you any answers to the problems but will be happy to try to clarify any confusion you may have, probably by asking you more questions. You may feel free to use any written references or books or even the internet, just no consultation with any persons.

As usual, you will be graded both on mathematical content and on clarity of expression. Each problem is worth a maximum of 12 points. Some of the questions are a bit open-ended, so be creative, make conjectures, and back up your assertions with a proof or a counterexample. In writing your answers, use complete English sentences and be sure to say exactly what you mean. Papers will be graded on the basis of what you have written, so be sure to take the time to express yourself clearly. If you are stuck on a problem and have no idea where to begin, a good way to get started is to look at lots of numerical examples and try to find a pattern.

On this test you again have a choice. Do any **five** of the following six problems. You must decide which ones you think you can do best. If you do all six, I will count only the first five—not the best five.

(1) Find the greatest common divisor of 3591874 and 4577419. Express this gcd as a linear combination of 3591874 and 4577419.

(2) Decide whether the integer equation $6603x + 5680y = -213$ has any solutions. If it does, find infinitely many solutions.

(3) Observe that for $n = 1, 2, 3, 4, 5$, the values of the expression $n^2 - n + 41$ are 41, 43, 47, 53, 61 — all primes. Is this always true? In other words, is $n^2 - n + 41$ a prime integer for every integer n?

Here's another one: for any integer $k \geq 1$ let let p_k be the kth prime; i.e., $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, etc. Is $(p_1)(p_2)\cdots(p_k) + 1$ always a prime number for any $k \geq 1$? For instance, when $k = 1$ we get $p_1 + 1 = 3$, which is prime. For $k = 2$ we have $(p_1)(p_2) + 1 = (2)(3) + 1 = 7$, which is also prime. For $k = 3$ we have $(p_1)(p_2)(p_3) + 1 = (2)(3)(5) + 1 = 31$, which is again prime. Will this always give us a prime number?

(4) For each of the following two integers, determine whether it is prime or composite. If prime, explain why you are sure it is prime and if composite, give its complete factorization into primes.
   (a) 17011
   (b) 17013

(5) Factoring big numbers is a very hard problem. But big numbers which have a very special form can often be completely factored into primes by using some algebraic tricks before doing trial divisions. Using the well-known factorizations of $a^2 - 1$, $a^3 - 1$, and $a^3 + 1$ to get a good start (look them up if you don't remember them), find the complete prime factorization of $7^{24} - 1$. (Note that $7^{24} - 1 = 191,581,231,380,566,414,400$ is a twenty-one digit number which you could factor by brute force trial divisions if your calculator carries enough

digits – most don't – but it would be a very tedious task using only the trial division method.) Hint: Go as far as you can without using this, but I will tell you that 193 is a factor.

(6) *Twin primes* are pairs of consecutive odd integers $(p, p+2)$ which are both prime. For example, $(3, 5)$, $(5, 7)$, $(11, 13)$ are all pairs of twin primes. Give three more examples of twin primes. The Twin Prime Conjecture (still unresolved) claims that there are infinitely many pairs of twin primes.

Building on this idea, we can define a set of "triplet primes" to be three consecutive odd integers $(p, p+2, p+4)$ which are all primes. A quick scan of our list of primes less than 100 shows that there is exactly one set of triplet primes in that range: $(3, 5, 7)$. Are there any other sets of triplet primes (ever)? If so, give an example. If not, prove that there are no others.

Statement of Sources: As this was a "Solo" exam, you shouldn't have talked with anyone besides the instructor about this exam. Please write the following statement on your exam, and sign your name:

I have neither given nor received any help on this exam.

Also, if you used any references besides the class notes, list them as well.

Appendix E. Take-Home Test 3

Due: Thursday, October 9

Collaboration Allowed

Collaboration on this test is both allowed and encouraged. By collaboration, I mean that you are encouraged to discuss the problems, test out your ideas, check your reasoning and arguments, etc., with other people. *However, there is a big difference between collaborating and copying. Each student must write up his or her own solutions to the problems in his or her own words.*

As before, you will be graded both on mathematical content and on clarity of expression. Each problem is worth a maximum of 12 points. In writing your answers, use complete English sentences and be sure to say exactly what you mean. Papers will be graded on the basis of what you have written, so be sure to take the time to express yourself clearly.

On this exam there are no choices. (Sorry!) Everyone must do all five problems.

(1) The **Fibonacci sequence** is a sequence of integers $a_0, a_1, a_2, \ldots$ which is defined as follows: $a_0 = 1$, $a_1 = 1$ and for all $n \geq 2$, $a_n = a_{n-1} + a_{n-2}$. Thus, $a_2 = 2$, $a_3 = 3$, $a_4 = 5$, etc. Prove that for all $n \geq 0$ we have

$$a_n \leq (\frac{1+\sqrt{5}}{2})^n.$$

(2) In class, we talked about the "E-Zone" — the set of even integers. Those integers which could not be written as a product of two even integers were called "E-primes".
   (a) Make a conjecture of the form "There will be precisely *three* different ways to factor the even integer n as a product of E-primes if and only if _____."
   (b) Prove your conjecture.

(3) Let x and y be integers and $n \geq 1$ an integer.
   (a) Note that $x^2 - y^2 = (x-y)(x+y)$ and $x^3 - y^3 = (x-y)(x^2+xy+y^2)$. Prove that for any $n \geq 1$

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y3 + \cdots + xy^{n-2} + y^{n-1}.$$

   In particular, if $x \neq y$ then $x - y$ divides $x^n - y^n$. (Note: You do not need to use induction on this problem!)
   (b) Prove that if $2^n - 1$ is prime (i.e., a Mersenne prime) then n must also be prime. (Hint: If $n = ab$ then $2^n - 1 = 2^{ab} - 1 = (2^a)^b - (1)^b$.)

(4) Let $a \geq 2$ and $n \geq 1$ be integers.
   (a) Prove that if $a^n + 1$ is prime then $n = 1$ or n is even. (Hint: Note that if n is odd then $a^n + 1 = a^n - (-1)^n$.)
   (b) Prove that if $2^n + 1$ is prime then n is a power of 2. (Primes of this form are called *Fermat primes*.)
   (c) Find the first three Fermat primes.

(5) For positive integer n, we define $n!$ to be $(n)(n-1)(n-2)\cdots 2\cdot 1$. For example, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$. By convention, we define 0! to be 1. Now let $n \geq k$

be two non-negative integers. The *binomial coefficient* $\binom{n}{k}$ is defined by

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

(a) Find $\binom{8}{2}$, $\binom{10}{4}$, $\binom{7}{5}$ and $\binom{12}{7}$.

(b) Prove that for all integers n and k such that $n \geq k \geq 1$

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

(c) Prove that $\binom{n}{k}$ is an integer for all positive integers n and all integers k such that $0 \leq k \leq n$.

Statement of Sources: : Give a list of all people with whom you discussed the problems on this test. Also, if you used any references besides the class notes, list them as well.

Appendix F. Take-Home Test 4

Due: Thursday, October 30

Solo – No Collaboration Allowed

All the usual instructions apply. Keep in mind that this is a solo exam and your work is to be your own with no consultation with any other person (in this class or not) except for the instructor. You may feel free to use any written references or books, just not any consultation with living persons.

Do **four** of the following five problems. If you do more than four, please be clear about which four you wish to count.

(1) (a) Prove that $38(7^{2n+1}) - 13(16^{2n})$ is divisible by 23 for all $n \geq 0$. (Hint: use congruences!)

(b) Is $3333^{4444} + 4444^{3333}$ divisible by 77? Hint: This will be easier if you notice that a number is divisible by 77 if and only if it is divisible by both 7 and 11.

(2) (a) Let a, b, n be integers with $n \geq 0$. Use induction and the result of problem 5(b) from Test #3 to prove the *Binomial Theorem:*

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots \binom{n}{i}a^{n-i}b^i + \cdots \binom{n}{n-1}ab^{n-1} + b^n$$
$$= \sum_{i=0}^{n} \binom{n}{i}a^{n-i}b^i.$$

(b) Prove that if p is prime then $\binom{p}{i} \equiv 0 \pmod{p}$ for $1 \leq i \leq p-1$.

(c) Let p be a prime and a, b integers. Prove *The Freshman's Dream:*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

(Yes, I *am* making fun of freshmen!)

(3) Find and justify a divisibility test for dividing an integer by 101 in terms of the digits in the base 10 representation of the integer.

(4) Let a, m be integers with $m > 0$. Let's say that *cancellation holds for the pair* (a, m) if whenever $ab \equiv ac \pmod{m}$ for integers b and c then $b \equiv c \pmod{m}$. So for instance, cancellation never holds the pair $(0, m)$ for any $m \geq 1$, while cancellation always holds for $(1, m)$. In class, we showed that cancellation always holds for the pair (a, m) if m is prime and $a \not\equiv 0 \pmod{m}$. What if m is not prime? Investigate this question for different values of (a, m), where m is not prime (e.g, $m = 4, 6, 8, 9$) and form a conjecture about when cancellation holds for the pair (a, m). That is, conjecture a condition that would finish the sentence "Cancellation holds for the pair (a, m) if and only if *blank*." Finally, prove this conjecture.

(5) (a) Let p be an odd prime. Prove that $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

(b) Let n be a positive integer such that $n \equiv 3 \pmod{4}$. Prove that n is divisible by some prime p such that $p \equiv 3 \pmod{4}$.

(c) Prove there are infinitely many primes which are congruent to 3 modulo 4. (Hint: Try to mimic Euclid's proof on page 35 of your notes. You may want to evaluate an expression of the form $(p_1^2 p_2^2 \cdots p_k^2 + 2)\,\%4$.)

Statement of Sources: As this is a "Solo" exam, you shouldn't have talked with anyone besides the instructor about this exam. Please write the following statement on your exam, and sign your name:

I have neither given nor received any help on this exam.

Also, if you used any references besides the class notes, list them as well.

Appendix G. Take-Home Test 5

Due: Thursday, November 13

Collaboration Allowed

Collaboration on this test is both allowed and encouraged. By collaboration, I mean that you are encouraged to discuss the problems, test out your ideas, check your reasoning and arguments, etc., with other people. *However, there is a big difference between collaborating and copying. Each student must write up his or her own solutions to the problems in his or her own words.*

As before, you will be graded both on mathematical content and on clarity of expression. Each problem is worth a maximum of 12 points. Some of the questions are a bit open-ended, so be creative, make conjectures, and back up your assertions with a proof or a counterexample. In writing your answers, use complete English sentences and be sure to say exactly what you mean. Papers will be graded on the basis of what you have written, so be sure to take the time to express yourself clearly. If you are stuck on a problem and have no idea where to begin, a good way to get started is to look at lots of numerical examples and try to find a pattern.

On this exam there are no choices (eek!). Everyone must do all five problems.

(1) For each of the following calculations show all your work. You may use your calculator to check your answer, but I should be able to follow all your calculations without a calculator by reading your solution.
   (a) Find $o_{193}(2)$.
   (b) Find $14^{3664}\,\%193$.
   (c) Find $57^{-1} \pmod{193}$.

(2) Consider the equation $10^{20000} = q(10^{100}+3)+r$ where $q, r \in \mathbb{Z}$ and $0 \le r < 10^{100}+3$. In this problem you will find the units digit of q.
   (a) Show that $q \equiv 3r \pmod{10}$.
   (b) Show that $r \equiv 10^{20000} \pmod{10^{100}+3}$.
   (c) Use that $10^{100} \equiv -3 \pmod{10^{100}+3}$ to show that $r \equiv 9^{100} \pmod{10^{100}+3}$.
   (d) Conclude that $r = 9^{100}$. (Justify your answer.)
   (e) Use (a) and (d) to find the units digit of q.

(3) (a) For each odd prime $p < 20$, find an integer a with $1 \le a \le p-1$ and $o_p(a) = p-1$. (It turns out that if p is prime there is always such an integer.) Be sure to show that it is indeed true that $o_p(a) = p-1$.
   (b) For each example you found above, compute $o_p(p-a)$. Again, be sure to justify your answers.
   (c) Make a conjecture of the form "If p is an odd prime and $1 \le a \le p-1$ and $o_p(a) = p-1$, then $o_p(p-a) =$ *(fill this in)*. Hint: There will be two formulas for $o_p(p-a)$, depending on whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$.

(4) Let a and m be integers with $m > 0$ and $\gcd(a, m) = 1$. Let $k = o_m(a)$ and consider the set

$$S = \{1, a, a^2, \ldots, a^{k-1}\}.$$

(a) For any $n \in \mathbb{Z}$ prove that a^n is congruent modulo m to an element of S.
(b) Prove that no two elements of S are congruent modulo m.
(c) Prove that $a^{k-1} \equiv a^{-1} \pmod{m}$.

(5) (a) Let p be prime and suppose $a^2 \equiv b^2 \pmod{p}$. Prove that $a \equiv \pm b \pmod{p}$. Also, give an example to show this can be false if p is not prime.
(b) Suppose $a^k \equiv 1 \pmod{m}$ and $a^\ell \equiv 1 \pmod{m}$. Let $d = \gcd(k, \ell)$. Prove that $a^d \equiv 1 \pmod{m}$.

Statement of Sources: : Give a list of all people with whom you discussed the problems on this test. Also, if you used any references besides the class notes, list them as well.

Appendix H. Take-Home Test 6

Due: Thursday, December 4

Solo – No Collaboration Allowed

All the usual instructions apply. Keep in mind that this is a solo exam and your work is to be your own with no consultation with any other person (in this class or not) except for the instructor. Feel free to ask me any questions. I won't give you any answers to the problems but will be happy to try to clarify any confusion you may have, probably by asking you more questions. You may feel free to use any written references or books, just not any consultation with actual persons.

This time you have a choice. Do any **five** of the following six problems.

(1) (a) How many positive integers are less than 3200 and relatively prime to 3200?
   (b) How many positive integers are less than 9600 and relatively prime to 3200? (Provide a sentence or two of justification here.)
   (c) Find the last four digits of $3^{2,394,592,093,230}$. For this part, be sure to show your work and to cite clearly any results you use. You may use your calculator to square, multiply, and divide but that's it. Show your work carefully, noting when and how you used your calculator.

(2) If n is the product of two distinct primes p and q, and we know the values of p and q, then we proved in class that $\phi(n) = (p-1)(q-1)$. Find formulas for p and q in terms of n and $\phi(n)$. Thus, if you know n and $\phi(n)$ (and you know n has the form pq) then you can factor n. Show that your method for finding p and q works by using the fact that $\phi(31325369) = 31313280$ to factor 31325369. Hint: Start by showing that, in general, if $n = pq$ with $p > q$ then $p + q = n - \phi(n) + 1$ and $p - q = \sqrt{(p+q)^2 - 4n}$.

(3) An investigative reporter came across the following message recently. He says that he was told it was encoded using something called RSA public key cryptography with keys $e = 3299$ and $n = 4171$. He has no idea what this means. Can you decode it for him? Be sure to explain exactly what you did to decode the message. (To save you some time, it may be helpful to have a calculator or a computer which can handle a large number of digits, although you can do this problem with nothing more than a TI-86. Incidentally, the 'mod' function on the TI-86 is highly erratic and may not give you the correct answer, so be careful!)

1214 0556 3545 4089 1604 1128 1631 0313 3205 1004 1490 3646

(4) Most of you conjectured on the last exam that if p is an odd prime and $o_p(a) = p - 1$, then $o_p(p - a)$ is either $p - 1$ or $(p - 1)/2$, depending on whether p is congruent to 1 or 3 modulo 4, respectively. Prove this statement. Hint: First prove that if $o_p(a) = p - 1$ then $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. (Problem 5(a) on Test #5 is helpful here.) Also, note that as $p - a \equiv -a \pmod{p}$, then $(p-a)^k \equiv (-1)^k a^k \pmod{p}$. Finally, show that $(-1)^{\frac{p-1}{2}}$ is -1 if $p \equiv 3 \pmod{4}$ and 1 if $p \equiv 1 \pmod{4}$.

(5) (a) Make a list of values of $\phi(n)$ for $3 \leq n \leq 50$.

(b) All the values of $\phi(n)$ in your list should be even. Explain why this is always true. In other words, explain why $\phi(n)$ is even for every $n > 2$.

(c) In fact, it should appear from your list that $\phi(n)$ is "usually" divisible by 4. State a conjecture of the form "$\phi(n)$ is divisible by 4 if and only if *(fill this in)*", where the blank is filled in with some conditions on the prime factorization of n. You can earn bonus points by proving part or all of your conjecture.

(6) There has been a great curiosity about numbers all of whose digits are equal to 1, that is, numbers of the form 1, 11, 111, 1111, etc. They are called repunits (*rep*eating *units*). We shall denote the repunit consisting of a sequence of n ones by R_n. A helpful observation is that

$$R_n = 11\ldots111 = \frac{10^n - 1}{9}$$

(a) Show that no repunit is divisible by 2 or 5. (This one's a gimme!)

(b) Show that there are infinitely many repunits which are divisible by 3.

(c) Prove that for each prime p except 2 and 5, there is some repunit R_n which is divisible by p. (Hint: Fermat's Theorem is very useful here.)

(d) Is it true that for each prime p except 2 or 5 there are infinitely many repunits divisible by p? Give a proof or a counterexample.

(e) (*Bonus Points*) Prove that for any positive integer m which is relatively prime to 30 there is a repunit which is divisible by m. (Hint: Euler's Theorem!)

Statement of Sources: As this was a "Solo" exam, you shouldn't have talked with anyone besides the instructor about this exam. Please write the following statement on your exam, and sign your name:

I have neither given nor received any help on this exam.

Also, if you used any references besides the class notes, list them as well.